The Center for International Security and Cooperation, part of Stanford University’s Institute for International Studies, is a multidisciplinary community dedicated to research and training in the field of international security. The Center brings together scholars, policymakers, scientists, area specialists, members of the business community, and other experts to examine a wide range of international security issues.
The U.S. Military and Civil Infrastructure Protection: Restrictions and Discretion under the Posse Comitatus Act

Gregory D. Grove

October 1999
Abstract

This article sets out the constraints of the Posse Comitatus Act of 1878 (the “Act”), which generally prohibits active enforcement of civilian laws by the military, and describes the discretion of the military commander to assist civilian law enforcement in protecting America's information infrastructure against computer-assisted attack. A primary purpose of this article is to help legal advisors to commanders and DoD civilian officials better understand the boundaries of command discretion so that commanders and officials can feel free to exercise proper command discretion to assist law enforcement according to military interests and their professional and personal ethics and ideals. Another primary purpose of the article is to appraise Congress of the Act, its prohibitions, and its application to assist in framing the policy debate about how to constrain or expand the discretion of commanders and other officials to most productively serve the American public.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part IV: Recommendations for Officials</td>
<td></td>
</tr>
<tr>
<td>The Conservative View</td>
<td>46</td>
</tr>
<tr>
<td>Policy</td>
<td>47</td>
</tr>
<tr>
<td>Operational Readiness</td>
<td>47</td>
</tr>
<tr>
<td>Public Response</td>
<td>47</td>
</tr>
<tr>
<td>Accomplishment of the Stated Objective</td>
<td>48</td>
</tr>
<tr>
<td>Defenses</td>
<td>48</td>
</tr>
<tr>
<td>Against Criminal Liability</td>
<td>48</td>
</tr>
<tr>
<td>Against Civil Liability</td>
<td>49</td>
</tr>
<tr>
<td>Summary</td>
<td>49</td>
</tr>
<tr>
<td>Part V: Conclusion</td>
<td>50</td>
</tr>
<tr>
<td>Notes</td>
<td>51</td>
</tr>
</tbody>
</table>
Introduction

The vulnerability of America’s information infrastructures—telecommunications systems, the distributed public computing environment of the Internet, private and government computer networks, and the North American power grid—and America’s growing dependency upon those infrastructures have recently drawn interest from the highest levels of government. President Clinton established the Commission on Critical Infrastructure Protection (the “PCCIP” or the “Commission”), headed by Gen. Robert T. (Tom) Marsh, USAF, Ret., to assess vulnerabilities and recommend remedial action. The Commission’s October 1997 report spurred the creation of a Critical Infrastructure Assurance Office (“CIAO”), a National Infrastructure Protection Center (“NIPC”), and ongoing efforts to develop and implement a National Plan to protect infrastructure. The president announced in January 1999 a $1.46 billion program to protect America’s infrastructures and charged the 1998 graduates of the United States Naval Academy at Annapolis to learn about information infrastructure threats and protect the critical military systems and economic base of the United States from hostile regimes, terrorists, and criminals enabled by new cyber technologies. Such military activity is not without complications; however: The Posse Comitatus Act generally prohibits direct active use of military personnel to enforce civilian laws. This article addresses that prohibition and the exceptions that permit military participation in civilian infrastructure protection.

What Is Vulnerable?

An interdependent, highly leveraged network of infrastructures and control systems moves America’s food and water, heats homes, permits timely emergency medical, police, and fire services, enables effective military command, control, and logistics, and turbocharges America’s economy. The PCCIP identified eight “critical infrastructures” upon which both the military and civilians depend: transportation, oil and gas production and storage, water supplies, emergency services, government services, banking and finance, electrical power, and telecommunications/information systems. All these infrastructures depend upon computer networks for control and coordination. Military computer networks also coordinate command,
control, military communications, and logistics systems. Integration of computing and communications systems into the processes that facilitate governance and commerce make computing, communications, and electric power networks attractive targets to criminals, terrorists, substate international actors, and sovereign nations, who may seek to use unauthorized control or disruption of these networks to serve their own purposes.9

Use of networks and dependence upon them are growing. Some expect that American and European Internet commerce will exceed $5 trillion by 2005.10 The fact that the Defense Information Systems Agency delivers 95 percent of its communications through public commercial lines establishes a significant and important military dependence on commercial infrastructures.11 In addition, computer-assisted troop deployment and cargo logistics are the norm for U.S. military operations. Most critical infrastructures are owned and controlled by private companies12 and despite growing use and dependence many maintain that top management devotes insufficient attention to eliminating vulnerabilities in those infrastructures and the networks that control them.13

The increasing interdependence of telecommunications, electric power, and computer networks amplifies vulnerabilities. Failures may “cascade” from power to communications and information systems, and from communications and information systems into transportation, urban and agricultural water supply, financial services, and other infrastructures. Internal dependence of the electric power grid upon itself may cause failures to “propagate” from one geographic area to another—an outage in one portion of a national power grid can unbalance and topple the system in areas geographically distant from the initial failure.14 In other words, the electric power grid generates and distributes electricity, but it also depends upon electricity to run properly, and large portions of the grid may become unstable if voltages in one part of the grid fall below tolerances. Trunk line and switch failures increase communications traffic on surviving links, a situation that may overburden remaining lines and switches and deny service to some users.

Even short failures of information infrastructure control systems may result in economic losses, and possibly loss of life. In a competitive marketplace, with alternative communications systems to carry diverted traffic, a five-hour fiber failure of an optic ring communications network would cause an estimated $750,000 to $15 million in lost revenue.15 Complete failure of a fully loaded transcontinental or transoceanic bundled fiber trunk, which carries long-haul communications traffic, could run as high as $1 million per second,16 though full loading would be rare and competing providers would likely possess spare capacity to permit continued communication.

To compound these vulnerabilities, intrusion into information systems and networks is, in its most sophisticated form, surreptitious. The most dangerous intruders do not leave a taunt or calling card once they have gone. An intruder with significant resources and patience, like a sovereign country, is more likely to secretly and slowly develop increasing access to and control over computers and networks in a target country, waiting to use that control in a manner that will repay the effort of years of network reconnaissance. The intent of the intrusion may be to gather intelligence or, perhaps worse, the ultimate consequences of the intrusion may not be realized until the intruder has reason to attack and can profit by disrupting computer and network operations or by manipulating or destroying data.
Why Involve the Military in Protection of Privately Owned Infrastructures?

The military services have a direct interest in continued availability of communications and other infrastructures. That interest is recognized by the power of the President to take full control of telephone and radio systems in time of war or emergency, a power actually exercised during World War I. Regulation of communications is tied closely to the potential for military use. Loss of computer-coordinated services would seriously erode military effectiveness. At a minimum, the Department of Defense ("DoD") should inform the federal government regarding wartime and emergency infrastructure needs and assist in developing plans to satisfy those needs.

In addition, the military may be able to assist in securing a more robust set of infrastructures. Often, the military controls equipment and trained personnel that are useful to satisfy needs outside its ordinary area of operations. In the case of infrastructure protection, the federal government and military were early users of computers, networks, and secure communications. Sharing the knowledge and expertise of specialized military personnel developed over decades of protecting our nation's military information and operations could help make information infrastructures less susceptible to monitoring, sensitive information compromise, and malicious attack.

There are constraints on military involvement, however. In 1878, Congress passed the Posse Comitatus Act (the "Act"), which generally prohibits active participation of the military in enforcing civilian laws. The Act has grown to symbolize a professional separation of the military from domestic political and civilian affairs. The military can, of course, meet and address a national security threat, consistent with guidance from civilian authority; nevertheless, military commanders are bound to remain within the lines drawn for them by the Act. Within those bounds, they may exercise discretion according to their professional ethics and good judgment. This article addresses the boundaries established by the Act and the relatively broad discretion of commanders in the context of military protection of America's information infrastructures.

Purpose of This Article

The remainder of this article will set out the constraints of the Act and describe the discretion of the military commander. A primary purpose of this article is to help legal advisors to military commanders and DoD civilian officials with command authority better understand the boundaries of that command discretion. With a solid understanding of the law, commanders and officials can feel free to exercise command discretion to assist in law enforcement according to military interests and their professional and personal ethics and ideals. Another primary purpose of this article is to apprise Congress of the Act, its prohibitions, and its application to assist in framing the policy debate about how to constrain or expand the discretion of commanders to most productively serve the American public.

Part I contains a detailed analysis of the Act and its exceptions. Part II considers possible legitimate military interests in civilian-owned and -operated infrastructures. Part II also discusses and resolves the complexities of the Act's prohibitions in the context of an investigation to determine the identity of an unknown attacker. Part III applies the Act to hypothetical activities by military personnel. Part IV provides a simplified and conservative summary of the Act's prohibitions and discusses considerations that may be important to an official facing a decision influenced by the Act. Part V summarizes and concludes. If government officials without legal training are reading this article, it may be best to start with Part IV.
and read the remainder of the article if deeper background is desired. Those who skip Parts I–III will bypass a detailed analysis that would assist in resolving difficult cases that are “close to the line” where an official believes it in the best interest of the military to remain actively involved in a case, but where the “conservative view” set out in Part IV would counsel against such involvement.

Part I: The Act, Its Interpretation, and Exceptions

The Act

“[T]he central purpose of the Act [is] precluding the military from supplanting or supplementing civilian authorities as primary instruments of law enforcement.” Historically, the sheriff could call upon the community to aid in the pursuit and capture of bandits and escaped prisoners and otherwise to execute the laws when he and his existing deputies were insufficient in number to meet the challenge at hand. When the sheriff assembled a posse, men above the age of fifteen were obligated to answer the call. Before the passage of the Act, military members were not excluded from that obligation. Today, the sheriff may still assemble a posse, but military members must generally be excluded from the sheriff’s call.

In 1878, precipitated by actions taken by Union Army soldiers stationed in the South during Reconstruction to enforce civilian laws, Congress passed the Posse Comitatus Act and amended it over time into its current form:

Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned for not more than two years, or both.

The Act generally prohibits the direct, active participation of military forces to execute civilian laws. Passive military participation in law enforcement is permitted. Indirect assistance is permitted. Statutory clarifications have helped to distinguish active and direct participation from passive and indirect participation. Courts have also developed tests to categorize military participation in law enforcement activities.

An Abbreviated History of the Act

After the Civil War, Union Army troops were employed to enforce the Reconstruction statutes in the South. Army troops guarded returning (election certification) boards during the 1876 Presidential election, supervised the election of delegates to Constitutional conventions, supervised the registration of voters, combated illegal alcohol manufacture, interfered with the operation of the Louisiana State Legislature, and suppressed a labor dispute. Some historians view the Union Army’s actions as abuses suffered by the South, others as an influence that was necessary to uphold federal law during Reconstruction. In any event, it is generally accepted that these and other actions by the Army during the period resulted in the passage of the Posse Comitatus Act of 1878. Judicial interpretation of the Act became
somewhat confused in the wake of military involvement in law enforcement activity at Wounded Knee, South Dakota, in 1973. Legislative exceptions, most notably in the 1980s after the Wounded Knee cases were tried and appealed, clarified congressional intent regarding the military’s role in law enforcement and elaborated upon the manner in which military forces may participate in law enforcement activities. Extensive discussion of the debates surrounding passage of the Act, the Wounded Knee cases, and legislative intent of statutes are available in other scholarly research and will not be treated in depth in this article.

A Professional Military

Over time, the Act grew in the eyes of some to symbolize the separation of civilian affairs from military influence. This separation, which has been described by the Supreme Court as “a traditional and strong resistance of Americans to any military intrusion into civilian affairs. . . .”, became so firmly a defining part of the American professional military force that the First Circuit observed in 1948 that the Act had become “an obscure and all-but-forgotten statute.” That observation is testimony to the fact that seventy years after the Act became effective, actions by the military of the type that inspired the passage of the Act were so rare that they had been all but forgotten. In fact, since that time some courts have noted that violations of the Act have been isolated enough to avoid a need to address violations with an exclusionary rule to render evidence gathered in violation of the Act inadmissible.

Commentary regarding the Act has frequently mentioned the subject of executive and judicial confusion over the exact scope of its prohibitions. Deep understanding of the Act is uncommon. Confusion is compounded by the prospect of criminal sanction. When an attorney acts to advise a client on compliance with a criminal statute (such as the Act), interpretation of the statute and recommendations on action are understandably conservative. The decades-long record of generally successful adherence to the Act is possibly an indicator not of deep legal understanding of the Act’s prohibitions, but instead of a pragmatic and conservative incorporation of a broad concept into military professionalism—separation of the civilian and military spheres.

The separation concept so incorporated is certainly broader than the prohibitions of the Act itself. In the United States, the professionalism of a military officer demands that he or she accept direction from duly elected and appointed civilian authority. Further, professionalism forbids the officer from tinkering with the mechanism or even fully participating in the process that selects civilian authority, even though that officer will be affected by the choice both as a citizen and as a federal employee.

But what of advice? Professionalism permits the officer to advise civilian authority of strategic, tactical, and operational concerns relating to military action. Such advice is contemplated by statute. In addition, unique training in the profession of arms makes military officers particularly suited to advise civilian authority in some non-military situations. For example, the court in United States v. McArthur recognized that “the movement of substantial numbers of civilian officers [in open country in the face of civil disorder] is a matter about which army personnel are peculiarly vested.”

When the need to accomplish a legitimate military objective arises or a request for military assistance arrives from civilian law-enforcement authorities, professionalism demands that the officer consider how to best accomplish the mission using means within his or her discretion and advise civilian authority regarding military capabilities available to contribute. Prudent exercise of discretion, considering professional concerns including operational readiness and public sentiment, may lead a commander to conclude that military equipment and
personnel are not the best tools to apply to a given law enforcement need. Nevertheless, the commander should be aware of the extent of the constraints of the Act, which define one of the boundaries on commander discretion.

Who Is Prohibited?

Expressly, the Act prohibits anyone (e.g., a sheriff, a prosecutor, federal marshal, or military commander) from using military members to execute the laws. As applied, the Act’s prohibition is tested against the acts of military members to determine whether those military members are executing the laws. No one has been criminally prosecuted for violation of the Act, but questions surrounding violations of the Act have arisen in other contexts.

The Act applies expressly to the Army and Air Force. It does not expressly apply to the Navy, but the secretary of the Navy has mandated compliance with the Act by Navy and Marine Corps personnel as a matter of policy. Title 10 of the United States Code, section 375, appears to prohibit direct Navy participation in certain search, seizure, and arrest activity, but an Act-related exception actually permits such activity. The Act does apply to members of the National Guard who are acting in federal service. The prohibition does not apply the Coast Guard, members of the Reserve force who are not on active duty status or inactive duty for training status, members of the National Guard who are under command of a governor (under Title 32 U.S.C.) or otherwise not in federal service, certain cadets, civilian employees of the military services when not under the command and control of a military officer, and active duty military members when off duty and acting in a private capacity.

**Three Tests: Red Feather, Jaramillo, and McArthur**

There are three commonly applied tests (hereinafter collectively the “Three Tests”) to determine whether the Act has been violated. Each of the three was developed by a different court, but all three tests arose from use of federal troops at Wounded Knee, South Dakota, in 1973. A conservative reading of case law would require that all three tests be satisfied to ensure that no violation of the Act had occurred.

The Three Tests, which were established by other cases, are described and elaborated in United States v. Yunis, a case in which America took jurisdiction over Lebanese defendant Yunis accused of involvement in the hijacking of a Jordanian aircraft in the Middle East. The first test, the Red Feather test, is “whether civilian law enforcement agents made ‘direct active use’ of military personnel to enforce the laws.” The second test, the Jaramillo test, is “whether ‘use of any part of the Army or Air Force pervaded the activities’ of the civilian law enforcement agents.” The third test, the McArthur test, is “whether the military personnel subjected citizens to the exercise of military power which was regulatory, proscriptive, or compulsory in nature.” The Yunis case applied these tests and held that there was no violation in military members assisting FBI investigators to find defendant Yunis in international waters and transport him from those extraterritorial waters to the United States.

Direct Active Use

The Act does not expressly distinguish between direct and indirect or active and passive use of military forces to execute the laws, but the Wounded Knee cases do draw such a distinction. “Direct active use” of military personnel to enforce civilian laws is prohibited by the Red Feather test. Direct active use can be distinguished from supporting or indirect use.
The court in Yunis cited United States Code title 10, sections 371–378, as provisions that “clarify and reaffirm the authority of the Secretary of Defense to provide indirect assistance to civilian law enforcement officials. . . .”

The Yunis court held that the following were “clear[ly] . . . not . . . direct active involvement. . . .” advising law enforcement personnel on their location and the location of defendant Yunis in international waters, short-distance transport of an apprehended criminal suspect from a law enforcement vessel to a long-range military transport vessel, supplying a criminal suspect with shelter, clothes, food, and medical care while being transported by military vessel, and transporting a criminal defendant from international waters into the United States. Even though personnel were required to operate the Navy equipment and vessels used to maintain location information and transport the criminal suspect, the court held that the assistance was “passive” and “indirect” furnishing of equipment, supplies, and services.

From these holdings we can surmise that in circumstances where it may be impractical or expensive for law enforcement (in the case of Yunis, the FBI) to provide long-range transport of an apprehended criminal suspect, the military may use a vessel, aircraft, or vehicle to transport the suspect. It is important to note that the defendant Yunis was apprehended by the FBI and was in the custody of the FBI at all times, even when he was on military vessels and aircraft.

Further examples of the active/passive distinction arise in Red Feather. Active roles include arrest, seizure of evidence, seizure of a person, search of a building, investigation of a crime, interviewing witnesses, pursuit of an escaped civilian prisoner, and search of an area for a suspect. Passive roles include mere presence of military personnel under orders to report on whether military intervention is or may become necessary, preparation of contingency plans to be used if military intervention is ordered, advice or recommendations given to civilian law-enforcement officers on tactics or logistics, presence of military personnel to deliver military material, equipment, or supplies, training law enforcement officials on the proper use and maintenance of military material, equipment, or supplies, and aerial photographic reconnaissance.

Pervasiveness

The Yunis court held that the FBI's use of military personnel did not “pervade the activities of the civilian authorities” under the Jaramillo test. The court stated that the interdiction operation was a civilian one, originating from within the FBI, and that “by its very nature, the operation required the aid of [the] military” because the location of the suspect in international waters meant that Navy support services were “necessary.” The court stated that the military gave support “under the direction of the FBI” and concluded that the military involvement was not pervasive. By the Yunis analysis, rendering “aid,” its synonyms “indirect assistance” and “support,” passes the Jaramillo test.

The pervasiveness analysis of the Yunis court permits us to infer that when a law enforcement operation originates from within a law enforcement agency, such as the FBI, and its conduct is directed by that law enforcement agency, the loan, furnishing, and operation of equipment, vessels, and vehicles to locate and transport criminal suspects is not pervasive. Direction is synonymous with control, and, in a military context, with giving orders. The court in United States v. McArthur nearly equates giving orders to pervasiveness and, therefore, offering recommendations or advice to non-pervasiveness.
Presumably, the result of the analysis would differ if military personnel were giving orders to law enforcement personnel or directing a law enforcement activity by making strategic decisions about an investigation or about apprehension or prosecution of suspects. The court in McArthur found military member activity non-pervasive even when the member testified that he had a “vote in final policy decisions.” The court determined that the member had an “inflated concept of his function and duties” but that did not prevent him from being borrowed for his advice “as a vehicle might be borrowed” for its ability to transport.

In sum, a pervasiveness analysis consists of two prongs: origination and direction. Origination is a decision to open an investigation with a law enforcement goal, and direction is control through the giving of orders. Under this analysis, DoD can observe illegal activity, either in the ordinary course of duty or as a passive, order-taking tool of law enforcement, and report findings to the FBI or another law enforcement agency. At that point, law enforcement officers must decide whether to originate a law enforcement investigation, and, if they do, they can request additional assistance from DoD so long as law enforcement officers give direction and the assistance requested is not otherwise prohibited. This pervasiveness analysis integrates nicely with the Red Feather test’s allowance of passive and indirect activity such as advice, loan of equipment, and reporting of relative “location.”

Regulate, Proscribe, or Compel

The Yunis court also elaborated upon the McArthur test, which prohibits the exercise of military regulatory, proscriptive, or compulsory power over civilians. The Yunis court stated that a regulatory power is one that “controls or directs,” a proscriptive power is one that “prohibits or condemns,” and a compulsory power is one that “exerts some coercive force.”

The Yunis court noted in its McArthur test analysis of the facts that defendant Yunis was under the exclusive control, authority, and physical custody of the FBI and that mere presence on a Navy vessel did not constitute control or direction. As to prohibition or condemnation, the court stated that the defendant was never confined by military personnel; instead, he was in the custody of the FBI and never in any “real way” subject to proscriptive powers of the military. Finally, the court stated that Navy personnel never exerted a coercive force against Yunis and characterized the location and transport of Yunis as “indifferent, passive and subservient to the FBI’s task.”

Naturally, there is substantial overlap between the McArthur, Jaramillo, and Red Feather tests. For example, the “control or direct” language of the Yunis opinion when applying the McArthur test overlaps with the “under the direction of” language when applying the Jaramillo test. Moreover, the court’s “indifferent, passive and subservient” description when applying the McArthur test overlaps Red Feather’s “passive role” permission.

Recognizing these overlaps and using the Red Feather and Jaramillo analyses to provide context for the Yunis court’s otherwise spare McArthur analysis and, further, applying common definitions for words used by the court, we can infer that so long as law enforcement personnel are making decisions and giving orders with respect to any criminal investigation or law enforcement activity, those law enforcement personnel are controlling and directing the investigation or activity. In addition, so long as law enforcement personnel retain custody of a criminal subject, that subject is under the proscriptive or compulsory power of law enforcement, not military, personnel. Finally, indifferent, passive, subservient activity is not compulsory; therefore, so long as military personnel act without substantial military interest in response to orders from law enforcement and without unsupervised initiative, there is no compulsion by military force. The McArthur court’s analogy of borrowing an active-duty
colonel for his advice as a vehicle might be borrowed for transportation seems an apt illustration of indifferent, passive, and subservient activity.91

In this context it should be noted that the McArthur court permitted military members to observe, advise, counsel, suggest, and even urge that specific actions be taken, so long as the decisions were made by law enforcement officials. One author when discussing the McArthur test commented that “the law requires a high threshold of military intervention prior to finding a violation [of the Act]”92 and that “[t]his test provides wide latitude for military involvement in law enforcement.”93 The McArthur approach has been adopted in military regulation.94

Observations Regarding Breadth of the Three Tests
Jaramillo considers pervasiveness, which requires “activities of the civilian authorities”95—an investigation. Red Feather considers direct, active use of military members to execute the law, which requires a law to enforce. McArthur considers whether a person is subjected to the regulatory, proscriptive, or compulsory power of the military, which assumes a law, but may require nothing more than the exercise of power.96

In one sense, then, Jaramillo may be seen as the narrowest test and McArthur as the broadest, though violations of the Act under Jaramillo are not necessarily a subset of violations under McArthur. It is possible, but purely speculative, that a violation could be found under a McArthur analysis if military members prohibited or compelled a civilian to comply with a military regulation improperly applied or a regulation that would be properly enforced by another federal agency, for example, a Federal Communications Commission (“FCC”) regulation.97 Finally, it is possible that an order that is unrelated to any law or regulation might be issued to civilians by military personnel.98 Such a baseless order might also be judged a violation of the Act, even though there is no “law” being enforced, particularly if the civilian party believed that the order carried the weight of law.

Integrating the Three Tests
With the complexities of these three tests in mind, we may begin to reduce the tests to their essentials for more convenient discussion. Under the Three Tests, as described in Yunis, prohibited activity is active, direct, pervasive in origination or military direction, regulatory by effect of military control or direction, proscriptive upon suspects through military custody, or compulsory through use of military members in a partial (i.e., biased, with an agenda), active, and commanding position. Permitted activity is passive, indirect, originated and directed and controlled by law enforcement officials, indifferent (i.e., unbiased, without stake in the outcome), and subservient.

These tests may be further collapsed by joining common threads, such as combining control and direction as “control,” collapsing origination into control, and collapsing command (the opposite of subservience) into control.99 The resulting test: Prohibited activity is active, direct, partial (biased), or controlling of a suspect or investigation; conversely, permitted activity is passive, indirect, impartial (unbiased), and non-controlling.

Implications of the Tests
Under the Three Tests, if military members are involved in law enforcement activity, a law enforcement agency must retain direct, active control over the activity and military members must assist indirectly and passively. Law enforcement personnel may use military equipment, facilities, and the special expertise of military personnel when similar law enforcement equip-
ment, facilities, or experts are nonexistent, unavailable, or impractical to bring to bear. Expertise in the form of proper and effective use of military equipment and suggestions that arise from special training or experience not possessed by law enforcement personnel may be shared by military members with law enforcement personnel, but significant initiative or strategic activity to advance an investigation or change its focus should occur under the direction of law enforcement authorities. A suggestion by a military member may lead law enforcement agents to change strategic focus or direction, but if the law enforcement agent in charge chooses to act contrary to the suggestion, military members have no power to require law enforcement personnel to adopt the suggestion. Military members should not give orders to law enforcement personnel, because that may constitute pervasive activity. Civilian suspects should be arrested and placed into custody only by law enforcement personnel, not military members.

The Impracticality Requirement

When military commanders determine whether to render passive, indirect assistance to civilian authority, they should consider the duration of the assistance and the resources already available to the civilian authorities to accomplish their law enforcement objectives. Assistance is improper if civilian authorities can readily accomplish the task at hand without such assistance. The shorter the duration and the more impractical it is for civilian authorities to train necessary personnel and purchase necessary equipment, the greater is the justification for military assistance. When active, direct law enforcement activity is permitted by an exception to the Act, as discussed below in the section on Statutory Exceptions, this requirement does not apply.

An impracticality requirement is not mentioned in the statute, but a conservative reading of the case law supports such a requirement. A legislative history analysis also provides support. Implementing regulation also embodies this requirement. In the Yunis case, it would have been impractical and expensive for the FBI to duplicate the equipment and expertise possessed by the military that was required to locate and transport the defendant in the open ocean. According to the Yunis court: “Among the legitimate governmental interests promoted by the use of military involvement in civilian affairs is the interest in improving the efficiency of civilian law enforcement by giving it the benefit of military technologies, equipment, information and training personnel.” Legislative history of statutes clarifying the Act limits “[military] assistance . . . to situations where the training of civilian personnel would be unfeasible or impractical from a cost or time perspective.”

A requirement for temporary duration arises out of the impracticality requirement. The longer the duration and more consistent the ongoing need for military assistance, the more practical it would generally be to establish a civilian capability to address that need. Temporary assistance during the interim for development of civilian capability is generally proper. Military training of civilian personnel to establish such a civilian capability is also proper.

The rationale for this impracticality requirement, and the implied temporary duration requirement, is avoidance of waste in government. If law enforcement authorities were required to train specialized personnel and maintain expensive military-grade equipment that would rarely be used, government would incur substantial unnecessary expense. If, however, civilian authorities routinely require such equipment or personnel on a permanent basis, those authorities should develop and maintain a capacity to meet such requirements.
Constitutional Roots but No Constitutional Right

Some courts have discussed possible Constitutional and Constitutionally antecedent underpinnings of the Act, which may suggest Constitutional guarantees to individual persons of freedom from military involvement in civilian law enforcement. That possibility should not be taken lightly, for military members must avoid treading upon the liberties established by the Constitution, particularly in light of each member’s oath “to support and defend the Constitution of the United States. . . .” Analysis yields the conclusion, however, that any rights that arise from the Act are statutory in nature and not Constitutional. While some cases feint at establishing a personal Constitutional guarantee, none of them hits the mark directly; and, in fact, authority supports a conclusion that no such Constitutional guarantee exists.

The court in United States v. Walden cited congressional debate supporting the position that the Act was simply a statutory codification of Constitutional limits on use of the military to enforce civilian laws. The Walden court also cited Laird v. Tatum, the Third Amendment’s prohibition against quartering of soldiers, and Constitutional provisions for civilian control of the military as support for “a traditional and strong resistance of Americans to any military intrusion into civilian affairs.” The court was careful to point out, however, that the “traditional American insistence on exclusion of the military from civilian law enforcement” is suggested by only some to be “lodged in the Constitution.” Walden does not, however, establish a personal Constitutional guarantee against military enforcement of civilian laws.

The court in United States v. Yunis suggested a possible Constitutional connection when it stated, “Limiting military involvement in civilian affairs is basic to our system of government and the protection of individual constitutional rights.” The existence or not of a Constitutional right is not necessary to decide the case, however, so the court’s isolated suggestive sentence is dictum; and, in fact, the court establishes no personal Constitutional guarantee in the course of deciding the case.

It may be that the rationale supporting the Act emanates from concerns reflected in the Constitution without giving rise to a Constitutional right. In Lamont v. Haig the court also cites the Laird “tradition of Anglo-American distrust of military involvement in civilian affairs.” After considering historical moments influenced by such distrust in military involvement, including “the Magna Carta, the Peasants’ Revolt in England in 1381, the struggle between Charles I and Parliament, the Boston M assacre, [the] Civil War, Reconstruction, [and] the 1876 Presidential Election. . . .” the court concludes that

none of the nineteenth century cases relied upon [to establish a Constitutional right for each person] make any discussion of any such constitutional guarantee; rather the most these cases do is support the familiar proposition that members of the military, like other public officials, are subject to suit for their individual commission of common-law torts.

In other words, according to the Lamont court, there is no Constitutional right against military involvement in civilian affairs.

In a later procedural appeal, the Eighth Circuit considered the Lamont court’s order to amend the complaint and determined that the Lamont plaintiffs had stated a claim under the Fourth Amendment by alleging that military members had unreasonably searched and seized their property. This holding, however, did not establish a Constitutional right against
military involvement in civilian affairs; rather, it provided that military members, like other
government employees, may be held accountable for violating well-established Fourth Amend-
ment rights.

The Walden court also reminds us that the Congress possesses as an enumerated power
the authority to “provide for calling forth the Militia to execute the laws of the Union, to
suppress Insurrections, and repel Invasions . . .” and the obligation to “guarantee to every
state . . . a Republican Form of Government . . . [to] protect each [State] against Invasion
and . . . against domestic Violence.”118 A personal Constitutional guarantee against military
involvement in civilian law enforcement seems inconsistent with this express Constitutional
permission for the federalized militia to execute the laws of the Union in accordance within
the provisions of Congress. This inconsistency appears particularly strong in light of the fact
that such a personal guarantee is not expressly described anywhere in the Constitution.

The Laird, Yunis, and Lamont courts describe a traditional policy of military separation
from civilian law enforcement, yet none of those cases recognizes a personal Constitutional
guarantee of freedom from military enforcement of civilian laws. In particular, the express
Constitutional authority of Congress to provide for military enforcement of civilian laws,
the lack of an express Constitutional prohibition against such enforcement, and the holding
of the Lamont court support the position that any such guarantee is statutory in nature and
not Constitutional.

Extraterritorial Application of the Act

Stealthy computer invaders cover their tracks and evade pursuit by weaving through com-
puter systems in many countries. Coordination of authorities in many jurisdictions with
different legal systems delays and often thwarts attempts to locate intruders. As of May
1999, no multilateral convention on information sharing for electronic pursuit exists, but
bilateral “Mutual Legal Assistance Treaties” (“MLATs”) already in place may assist officials
in different countries decide in advance how to cope with “hot pursuit” of electronic intrud-
ers across sovereign boundaries. In the absence of MLATs, personal relationships between
government officials of all kinds, including military officials, may be helpful in expeditious
resolution of requests for information. Military personnel may also desire to pursue or track
an intruder outside the boundaries of the United States. The question of applicability of the
Act to extraterritorial law enforcement activity by military personnel then arises.119

In general, domestic laws do not apply outside the borders of the United States, unless
Congress manifests its intent for extraterritorial application.120 Such application of a domes-
tic law would be unusual, and therefore silence on the issue of extraterritorial application is
presumed to indicate the negative intent of Congress. Such a presumption is overcome only
when the subject matter of the law is “inextricably linked to international interests”121 or
where the prohibition overlooks the occasions where the law would “most likely” apply.122

When presented with the issue of extraterritorial application of the Act in occupied Ger-
many after World War II, the court in Chandler v. United States stated, “[T]his is the type of
criminal statute which is properly presumed to have no extra-territorial application in the
absence of statutory language indicating a contrary intent.”123 The nonapplicability of the
Act in occupied territory rests in large part on the authority of an occupying force under
international law to exercise the powers of the sovereign required to maintain law and order
in occupied territory.124 In addition, an analysis of congressional intent supports a position
that the Act is not applicable to extraterritorial use of military force during wartime.125 Some
regulation adopts the view that the Act does not apply at all outside the continental United States, although that view may be too permissive.

A complete discussion of extraterritorial application is beyond the scope of this paper. Scholars who have more closely examined extraterritorial law enforcement by United States military members have concluded that extraterritorial application of the Act is limited. Two scholarly treatments summarize their findings on extraterritorial application:

Although not completely meaningless, the Posse Comitatus Act seems to be of greatly reduced concern in an international context. Within the framework of American statutory law, it is proper for the President to use the military to enforce domestic laws abroad as long as the action does not conflict with the reach of civilian authority. Even if there is such a conflict, use may be permissible if the action is explicitly approved by Congress or undertaken on an emergency basis by the President. From a strictly operational standpoint, American domestic law permits [extraterritorial] law enforcement by the military.

With respect to actions by the executive branch where the primary purpose or effect is to further United States foreign policy or to protect American lives or property overseas, the Act should not be given extraterritorial effect. The use of military personnel outside the United States for purposes of assisting domestic law enforcement when there is not substantial foreign policy interest presents a more difficult question.

Other practical, political, and diplomatic implications may restrict extraterritorial law enforcement, including international relations, military readiness, and effects on America’s reputation for respecting the principles of international comity and national sovereignty.


Active, direct law enforcement by military members is permitted under the Act when such activity is “expressly authorized by . . . act of Congress.” Therefore, statutory descriptions of permitted military activity constitute exceptions to the Act’s prohibitions.

The Uniform Code of Military Justice

A most obvious and venerable exception to the Act is the Uniform Code of Military Justice (“UCMJ” or the “Code”). The Code permits investigation, prosecution, and punishment of certain crimes committed by military members. Investigations, interrogations, arrests, searches, seizures, and other related activity may all be completely controlled and directed by military personnel if a perpetrator of crime is subject to the UCMJ. If a military member, or other person subject to the Code, attacks or otherwise compromises military or civilian information infrastructures, military jurisdiction attaches. Military investigators may interview civilian witnesses. Military trial counsel may exercise federal subpoena power over persons and physical evidence. Notwithstanding this authority, military investigators should coordinate with civilian law-enforcement officials when military perpetrators have civilian accomplices.

The Drug/Customs/Immigration Exceptions

A more recent set of exceptions, which became effective in 1981, was passed by Congress to clarify permitted military assistance to civilian law enforcement in the areas of drug interdic-
tion, customs, and immigration. The exceptions permit the sharing of information and intelligence,\textsuperscript{135} the loan of equipment and facilities to law enforcement,\textsuperscript{136} the provision of training by military members to law enforcement officials,\textsuperscript{137} and maintenance and limited operation of loaned equipment by DoD personnel.\textsuperscript{138} Military personnel operating DoD equipment loaned to law enforcement may only "monitor and communicate the movement of air and sea traffic";\textsuperscript{139} however, when "the size or scope of the suspected criminal activity poses a serious threat to the interests of the United States" and "serious[] impair[ment]" of federal drug, customs, or immigration law is threatened, military assistance can be expanded.\textsuperscript{140}

The 1981 statutes also prohibit direct military search, seizure, and arrest of civilians.\textsuperscript{141} This can be seen as an extension to the Navy of the Red Feather court’s prohibition of direct law enforcement, such as arrest, seizure of evidence, seizure of a person, search of a building, investigation of a crime, interviewing witnesses, pursuit of an escaped civilian prisoner, and search of an area for a suspect.\textsuperscript{142} However, these statutes constitute only clarifications of military authority under the Act.\textsuperscript{143} In the view of one scholar, under a non-preemption provision contained in the statutes, any activity that was permitted before the statutes remains lawful—\textsuperscript{144} the statutes were not intended to limit activity by the military; rather, they were intended to clarify the permissible role of the military under the Act. That author concludes that since active, direct enforcement was permitted under the Act before the 1981 statutes, the statutes do not prohibit such Navy activity. The Navy has not, however, availed itself of this logic. Navy regulation forbids the activity, even if the statute does not.\textsuperscript{145}

Nevertheless, the statutes provide a strong confirmation of the principles of the Red Feather test as described above.\textsuperscript{146} The fact that the 1981 statutes were intended to clarify the existing state of the law encourages application of the principles of the statutes outside the narrow contexts of drug interdiction, customs, and immigration enforcement. Generally speaking, loan of equipment and facilities, training of law enforcement officials, maintenance of equipment, and operation of equipment to passively monitor and communicate are permitted. These principles reconfirm the above analysis under the Three Tests.

Other Statutory Exceptions

Other notable statutory exceptions include those that permit the President to employ military troops to suppress insurrection\textsuperscript{147} and those that permit the military to protect certain federal officials,\textsuperscript{148} assist the Secret Service in their protective details,\textsuperscript{149} and assist when Americans are taken hostage.\textsuperscript{150} Another set of exceptions permits military personnel to investigate the threat or use of biological, chemical, and nuclear weapons.\textsuperscript{151} A litany of more than a dozen other special-purpose exceptions enacted during the Act’s effectiveness is contained in scholarly research and regulation.\textsuperscript{152}

The Emergency Exception

Emergency is the basis of executive-branch authority to act under the justification of necessity.\textsuperscript{153} Ordinarily, the employment of troops to control a civil disturbance requires authorization of the President; however, where an exigency is so urgent that delay to check with higher authority could endanger human life or result in wanton destruction of property, a local commander can act in his or her best judgment to preserve life or property, and that activity will not violate the Act.\textsuperscript{154} If the decision is a bad one, a commander may be held accountable by his or her superiors, so if at all possible the commander should attempt to get approval or at least seek the opinion of legal counsel; however, if lives really are at stake and
advance approval is impossible, taking necessary immediate action while concurrently seeking approval may be best.

This emergency exception, a justification of necessity, may explain why John Deutch, former deputy secretary of defense and former director of the CIA, concluded that the Posse Comitatus Act was not a barrier preventing military response to a genuine threat, but rather a bureaucratic reason not to do something perceived as less than a genuine threat. Military resources are limited, and commanders must accomplish many tasks. Shepherding resources to ensure military readiness is important, but if a grave infrastructure security compromise threatened the lives of Americans, commanders from the local level to the President could respond to the emergency with all available resources including military personnel.

Support for emergency authority in addition to a defense of justification may also be gathered pursuant to the President’s Constitutional obligation to “take Care that the Laws be faithfully executed.” To fulfill that obligation the President may call upon federal troops as necessary in emergency situations to execute the laws. Some scholars call this Presidential obligation and corresponding power the “inherent authority of the Executive.”

Temporary use of troops to fill a gap in civilian authority forces may be justified under the emergency exception. For example, a situation that threatens human life or wanton destruction of property may arise where the local police force is simply insufficient in number to protect the public. If, for example, the state police force cannot respond for six hours and the National Guard cannot respond for twenty-four hours, troops from a local military base may assist local law enforcement until relieved in six hours by state police, and if the state police prove insufficient, troops may remain until relieved by National Guard troops. If the National Guard is insufficient, a catastrophe justifying the attention of the President and a formal declaration of emergency may exist. In these stopgap situations, federal troops should be employed on a temporary basis and only until they can be relieved. If such stopgap situations occur routinely, civilian authority should retain and train additional law enforcement personnel to handle such occurrences. They should not rely on federal troops, because such an “on-call” use would not be temporary.

The Military Purpose Exception
When the purpose of an action taken by military members is primarily to pursue a legitimate military interest, the action falls into what may be called a military purpose exception to the Act. For example, military personnel may investigate loss of household goods of a military member in a commercial warehouse due to fire or theft when they are stored under government contract. They may investigate claims against the government and share information in the course of such an investigation with civil authorities. Troops may also guard military exchange funds in transit and direct traffic to preserve the integrity of a military convoy traveling off base.

Existing scholarly analysis has discussed the military purpose exception at length. Furman comments that the Act is limited to deliberate use of armed force for the primary purpose of executing civilian laws more effectively than possible through civilian law enforcement channels, and that those situations where an act performed primarily for the purpose of insuring the accomplishment of the mission of the armed forces incidentally enhances the enforcement of a civilian law do not violate the statute.
Meeks summarizes the holdings of administrative opinions related to military purpose:

Many law enforcement activities performed by military officials benefit the civilian community as well as the military command. This dual purpose “execution of the law” can, and often does, violate the Act. Where the primary purpose of the action is to fulfill a legitimate military requirement, no violation of the Act occurs even though civil law enforcement is incidentally aided. However, where action by military officials is taken primarily in aid of civil authorities, the Act is violated even though the military command is aided incidentally.167

Distillation of precedent and commentary yields a “primary purpose” test. Where the pursuit of a legitimate military interest is the primary purpose of military efforts, active, direct law enforcement by military members is permitted. Where the military interest is only incidental to the civilian purpose, such enforcement is prohibited.168 Protecting military systems and networks, performance of ordinary duties, and investigating military member misconduct are all legitimate military interests. The military purpose exception forms a critical part of the legal foundation for and a primary limitation upon military participation in civilian infrastructure protection, as explained below in Part II. Exemplar legitimate military interests are discussed and applied to possible military actions below in Part III.

Summary

The Act prohibits military members from law enforcement that is active, direct, pervasive of civilian law-enforcement organizations, partial (biased), or controlling of a suspect or investigation. The Act also prohibits non-military personnel from using military members in such a manner. The Act does not apply directly to the Navy, but Navy regulation commands sailors and marines to comply with the Act’s prohibitions. Exceptions exist, including exceptions for investigation of crimes by military members, for emergency assistance when human lives are in danger, and for use of military equipment and expert military advice. The most important exception in the information-protection context is the military purpose exception, which, as will be explained in Part II, permits military members to investigate network attacks from an unknown source.

Part II: Military Ties to Civil Infrastructures

The Clear Responsibility of DoD

Presidential Decision Directive 63, issued in May 1998, clearly establishes that “[e]very department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems.”169 By this executive directive, DoD is clearly charged with protecting its own computer networks, communications, and other information systems.170 Preparing for, preventing, deterring, responding to, and reconstituting after an attack on such DoD-owned and -controlled information infrastructures is proper, so long as applicable regulation and civilian guidance are observed.171 Further, local
commanders are responsible for government property under their control and must act appropriately to protect such property.¹⁷²

**Military Purpose and Civilian Networks**

Some, but not all, military activity to protect civilian information infrastructures would qualify as primarily military and incidentally law enforcement related (or entirely unrelated to law enforcement). It is important, then, when examining a proposed military action, to ask if the military purpose or the law enforcement purpose of that action is primary.

**National Security or Law Enforcement?**

The military may legitimately address national security threats. 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 may be invoked.¹⁷³ A threshold question, then, when examining military action in light of the Posse Comitatus Act is whether the military action primarily addresses a national security threat or a criminal law enforcement matter.

In the course of pursuing its enduring national security goals and vital national interests, the United States encounters conflict and threats of conflict. The primary task of the U.S. military is to deter conflict if possible, or prevail in conflict that cannot be deterred or prevented.¹⁷⁴ Joint Vision 2010, the view of the Office of the Chairman of the Joint Chiefs of Staff on the future capabilities, needs, and function of America’s military services, states:

> America's enduring goals include: protecting the lives and safety of Americans both at home and abroad; maintaining the political freedom and national independence of the United States with its values, institutions, and territory intact; and providing for the well-being and prosperity of the nation and its people.

> These goals, in turn, generate American interests which must be protected and advanced. Our fundamental interests lie in enhancing US security, promoting prosperity at home, and promoting democracy abroad. . . . ¹⁷⁵

> American national security rests upon the ability to continue to achieve enduring goals and fulfill vital national interests. A threat to those enduring goals or vital interests is a national security threat. Military force, military preventive measures, and military deterrent effects are three of the tools that can be used to protect national security and continue to achieve enduring goals and fulfill vital interests.

> If a U.S. military action seeks to address a national security threat in a manner consistent with the direction of civilian oversight and assigned military objectives, that action is not primarily a law enforcement activity. In order to qualify as an action taken to promote national security, such an action should be rationally related¹⁷⁶ to a threat to the enduring goals or vital interests of the United States. Small actions, even removed from combat, such as ensuring proper operation of the telephone used to coordinate the transportation of food to support soldiers who are training for combat, can and certainly do qualify as promoting national security; however, it is perhaps better to work from big concepts down to small actions in making a rational connection between national security and actions to protect civilian information infrastructures.
Military Command and Control Depends upon Information Infrastructures

Military command and control ("C2") is “[t]he exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. . . .”177 According to the United States Joint Chiefs of Staff, “C2 is, perhaps, the single most important function in military operations.”178 Military operations are critical to protect national security. Such strong words link the viability of military operations to effective command and control, and thereby link command and control to national security. The Joint Chiefs continue, “Information superiority . . . is the key enabler for the C2 function. Optimum C2 . . . will depend on seamless communications. . . .”179 Here, strong words link C2 to information superiority and seamless communications, thereby linking communications and information superiority to national security.

Joint Vision 2010 presents four new operational concepts that it predicts will help the United States keep its military edge180 and foresees a tremendously important role for information and communications technologies in employing these warfighting concepts.181 A follow-on Joint Chiefs of Staff publication, Concept for Future Joint Operations: Expanding Joint Vision 2010, returns repeatedly to the necessity of “information superiority” as an enabler for all of the new warfighting concepts introduced in JV 2010.182 EJV 2010 posits that “[p]rotecting the effective operation of one's own information systems, and exploiting, degrading, destroying, or disrupting the opponent's will become a major [military] operational focus.”183 Indeed, the “uninterrupted flow of information” is one of the three components of information superiority.184 Protecting information infrastructures relevant to military operations is an important component of information superiority and is therefore rationally related to national security.

Many civilian-owned and -controlled networks are relevant to military operations. Both JV 2010 and EJV 2010 expect that military cooperation with civilian communications service providers will be required to robustly implement technologies and plans to permit the U.S. military to achieve information superiority in time of conflict.185 In fact, 95 percent of Defense Information Systems Agency ("DISA") communications flow over commercial networks.186 One net assessment expert estimates that 60 percent of all American military traffic flows through commercial networks.187 Since DISA is a primary handler of military communications, protection of the networks that carry such a preponderance of military traffic should be a significant military priority. Accordingly, the Joint Chiefs of staff expressly include “commercial communications systems used to transmit DoD data” in the Defense Information Infrastructure ("DII").188 America’s Joint Chiefs of Staff further recognize the importance of commercial networks in their definition of information infrastructures: “[I]nformation infrastructures are [l]inkages of individual information systems . . . that transcend industry, media and the military and include both government and non-government entities.”189

In particular, defensive information warfare will involve protecting the uninterrupted ability of American military forces to communicate on commercial networks. The offensive information-warfare operations of adversaries will leverage the impressive speed and connectivity of modern global networks against the United States, leaping the static lines of battle and flashing through physical barriers erected at America's geographic borders to strike at information infrastructure targets “in the rear.” Near-instantaneous globe-spanning attacks against civilian-owned assets supporting military operations are a contingency that American military forces should legitimately prepare for. Protection of such commercial information infrastructure assets is therefore related to national security.
The foregoing analysis establishes a rational relationship between DII commercial information infrastructure assets and national security. Such a relationship gives rise to a legitimate military interest in protecting those civilian-owned and -operated assets. If the pursuit of that military interest is the primary purpose of a law enforcement activity by military personnel, the activity is permissible.

The Role of Civilian Law Enforcement

The Federal Bureau of Investigation has been charged to contribute to America’s infrastructure protection efforts through its National Infrastructure Protection Center. Presidential Decision Directive 63 orders government agencies to develop and implement plans to reduce the incidence and severity of infrastructure compromises.\textsuperscript{190} The Presidential mandate for the FBI’s NIPC includes uncovering vulnerabilities and detecting, warning of, investigating, and responding to computer-assisted intrusions.\textsuperscript{191} The NIPC will also coordinate emergency response.\textsuperscript{192} The FBI is also lead response agency for domestic counterterrorism.\textsuperscript{193} The Department of State coordinates response to international counterterrorism against U.S. targets.\textsuperscript{194}

Generally speaking, however, the FBI and state and local law enforcement agencies work to deter violations of federal and state criminal statutes and, when deterrence fails, to investigate, apprehend, and prosecute suspects. And again, generally speaking, it is this type of activity (investigating, apprehending, interrogating, prosecuting, and punishing civilians) that the Act prohibits military members from undertaking.

Cooperation between DoD and Law Enforcement

While speaking at Annapolis in May 1998, President Clinton urged the cooperation of the armed forces with law enforcement, intelligence, and other federal agencies under the coordination of the National Coordinator for Security, Infrastructure Protection and Counterterrorism\textsuperscript{195} “to bring the full force of all our resources to bear swiftly and effectively” upon threats.\textsuperscript{196} In accord with this view, President Clinton’s mandates in PDD 63 expressly contemplate cooperation among all government agencies including the FBI, DoD, and the intelligence agencies to achieve and maintain critical infrastructure protection.\textsuperscript{197} PDD 63 requires DoD to provide assistance, information, and advice to NIPC as requested and share information about infrastructure threats and attacks with NIPC, to the extent such assistance and sharing are permitted by law.\textsuperscript{198} The FBI is lead government agency for investigating crimes committed against U.S. government property or military installations.\textsuperscript{199}

Computer intrusion investigations may be beyond the experience of many state and local police forces. Most local police agencies do not actively pursue leads on computer security breaches.\textsuperscript{200} The FBI’s NIPC has specially trained investigators, as do some other federal, state, and large city departments, but “generations of police officers accustomed to following evidentiary paper trails may find chasing electronic data trails very difficult.”\textsuperscript{201} The accumulated knowledge of military defensive information-warfare organizations regarding damage control and methods to trace sources of attack could be very productive to the FBI and other law enforcers. For example, the Air Force Office of Special Investigations has a long history of detecting, thwarting, and tracking computer intrusions in both criminal and counterespionage situations.\textsuperscript{202} Expert advice and recommendations in the form of sharing practical knowledge about detecting intruders and tracking intrusions would be prudent to avoid expenditure of government resources in duplicative research efforts, and permissible under the Act.\textsuperscript{203}
Where the military can assist law enforcement passively and indirectly in the course of ordinary operations, Congress has contemplated that the military should coordinate with law enforcement to promote “compatible mission planning and execution.” In United States v. A. Hartley, the court found no violation of the Act when a United States Customs Service agent flew space-available on a military Airborne Warning and Controls Systems (“AWACS”) training mission to spot suspicious aircraft traffic crossing into American airspace. The “ride-along” was passive and indirect because the military purpose was primary and the law enforcement purpose was incidental.

Cooperation is permissible under the Act, and required by Presidential directive. Once military services gather information relevant to civilian law-enforcement investigations, cooperation and sharing must occur. The extent of permitted military activity to gather information during and following a computer-assisted infrastructure attack is discussed below.

The Uncertainty Problem

Even given President Clinton’s clear mandate for DoD to protect its own cyber systems, actions taken to protect military computers and networks may have impermissible civilian law-enforcement implications. An unidentified intruder into a military system could be an American civilian, over whom the military would generally not possess law enforcement authority, breaking federal criminal law against computer intrusion. Unfortunately, when military defenders of DoD systems routinely monitor system firewalls and respond to security incidents in the ordinary course of their duties, there is often no way for them to know the source (domestic or foreign) and purpose of the attack. Sophisticated attackers can make a domestic attack appear to originate overseas and vice versa. To complicate matters, when a “civilian” company is targeted, the purpose could be to discover military vulnerabilities, a possible motive when the target is a government contractor.

Seeking the identity of an attacker and that attacker’s organizational affiliation and citizenship may be as simple as tracing audit logs stored by computer operating systems and defensive information-warfare tracking programs; however, sophisticated attackers use camouflage tools like RootKit to cover their traces and hide a continuing intrusive presence in compromised systems. An attacker will frequently obfuscate the audit trail by weaving an electronic approach through many countries and many computers before launching a final attack. Involving multiple sovereign jurisdictions complicates tracking with international legal hang-ups. For example, in early 1998, investigators worked at least six weeks in an international backtrack to locate the source of an attack on DoD computers commonly referred to as “Solar Sunrise.” Later, in what was considered a rapid resolution, the March 1999 investigation surrounding the “Melissa” macrovirus uncovered the source of virus distribution in one week. These cases illustrate the present lack of real-time tracking capability from target to source, especially considering the commentary on the failure of those intruders to use available measures to evade detection. With tools like RootKit to amend audit trails and erase electronic traces of passage after the connection is closed, sophisticated attackers are safer from pursuit.

In theory, distinguishing between national security and law enforcement in this context may be possible. In theory, if one knew the identity and purpose of the attacker, one could make a determination of whether the attack was primarily a national security concern or primarily a law enforcement concern. In practice, however, a problem arises in distinguishing a national security threat from a crime in progress. In practice, intruders feel their way
through networks, breaking in surreptitiously and leaving behind RootKit\textsuperscript{217} and “sniffer”\textsuperscript{218} software to cover their tracks and gather information. Over time, a sophisticated intruder may secretly capture control of many computers and possess the capacity to disrupt the operation of the assets that rely upon them.

A savvy sovereign intruder may hold the keys to disruption yet wait months or years before acting, expanding its influence and waiting for the time when those months or years of computer reconnaissance can be strategically leveraged, perhaps to thwart an air strike, disrupt troop deployments, embarrass a diplomatic adversary, or divert attention from an international issue toward internal infrastructure difficulties. Unfortunately, sophisticated criminal intruders out for personal gain, revenge, or adventure operate in the same way and use the same tools to intrude, gather information, and cover their tracks. Criminals may also slowly and secretly expand their influence, awaiting the time when the advantage can be best used. Preventing and repelling such gradual infiltrations is extremely important. Gradual infiltrations permit intruders to acquire a platform to attack from inside the target and are therefore more effective than attacks from the outside.\textsuperscript{219} Stopping intruders before their motives can be determined will be required in some cases.

In remarks to a group of gathered scientists, policy scholars, and lawyers, Attorney General Janet Reno described the uncertainty problem and its implications for the military:

In the early stages of a cyber attack on an infrastructure . . . we often have no way of knowing who is behind it, what their motive was, or where they attacked from. It is impossible to determine whether the attack is part of a terrorist plot, a probe by a foreign intelligence service, or a part of a national-level military assault by a hostile nation state [or] simply the work of a disgruntled insider . . . [or] a young hacker out to test his skills against the latest firewalls.

At the outset [of a detected intrusion] . . . it may be premature to mobilize the military or redirect national intelligence assets . . . [R]egardless of the perpetrator, his intent or his whereabouts, the intrusion in most cases constitutes a federal crime. This means the Department of Justice and the FBI have the authority and responsibility to investigate it. . . .\textsuperscript{220}

Attorney General Reno continued, describing necessary coordination with the intelligence community and DoD during the course of investigations involving non-U.S. persons or hostile sovereigns, respectively. She also speculated that coordination may be appropriate with the National Security Council and the State Department in some circumstances.\textsuperscript{221}

Attorney General Reno’s remarks imply that as DoD goes about its business of “protecting its own critical infrastructure”\textsuperscript{222} it will encounter intrusions which “in most cases constitute[] federal crime[s].”\textsuperscript{223} Therefore, national security concerns will almost certainly overlap with law enforcement investigations, and such an overlap will implicate the Posse Comitatus Act. Out of the overlap will come issues regarding detection of attack, handoff of information from DoD to DOJ and FBI investigators, and the rendering of cooperation and assistance by DoD to DOJ and FBI investigators during their investigations.
Using an O'Callahan Analogy to Resolve the Uncertainty Problem

The discussion in this section draws an analogy to a body of case law that has been overruled. The logic underlying the analogy, which permits a commander to act in the face of uncertainty, is unrelated to the overruled point of law. Therefore, that logic, set out below, remains useful and valid. First, the overruled point of law is discussed to introduce the logic of resolving a commander’s dilemma resulting from a legal uncertainty related to the Posse Comitatus Act. Then, the logic is applied to the Posse Comitatus Act dilemma associated with infrastructure attack uncertainty.

O’Callahan v. Parker, now overruled, established that military members were not subject to prosecution under the UCMJ for offenses committed off a military base, unless the crime was service-connected. The proper forum for such non-service connected crimes was the civilian criminal court system. Occasionally, however, a military investigator faced uncertainty regarding whether an off-base crime was service-connected. In commentary, Meeks described this “commander’s dilemma” by stating that while military involvement might have been proper, “any military involvement such as apprehension or detention of the offender or investigation of the case may actually be aiding the civil authorities and consequently [be] a violation of the Act.”

Meeks’s analysis draws upon the “incidental” language discussed above in relation to the military purpose exception and upon the “active direct” language of the Red Feather test. Meeks asserts that if in fulfilling the obligations to pursue service-connected crimes, a commander “incidentally aids authorities, he has not violated the Act.” Then, by applying Gosa v. Mayden, which holds that O’Callahan did not establish a definitive jurisdictional boundary between civil and military courts, Meeks reasons that “military investigation of an off-base crime is not improper until it becomes clear that the civil forum is preferable under judicial guidelines . . . .” Therefore, “[i]f the commander continues active participation in the case after it appears that civil courts will be the more appropriate forum, then he has run afoul of the Posse Comitatus Act’s prohibitions.”

Meeks’s concept of discovering the appropriate forum invites analogous reasoning to resolve the infrastructure protection uncertainty problem. The commander’s dilemma regarding UCMJ applicability and military authority in the face of uncertainty about the service-connectedness of a crime is similar to a commander’s dilemma regarding primary military purpose applicability and military authority in the face of uncertainty about the source and purpose of an infrastructure attack. Hence, when an unknown attacker with unknown purpose commences an attack against a military computer, military members can expel the intruder, as common sense would dictate, even if that action gathers evidence that may later be used in a criminal prosecution. Moreover, military defenders may investigate the intrusion, both to prevent future intrusions and to determine the source and purpose of the attack. Once it appears that the civil courts will be the more appropriate forum, DoD must share the results of its investigation with the FBI or other appropriate law enforcement officials, identify and locate the individuals responsible, if possible, on the basis of the information DoD already possesses, and permit law enforcement officials to take “control” and determine whether to “originate” a law enforcement investigation.

So long as the investigation primarily addresses a situation that could reasonably be a national security threat, continued active participation by military members is proper. If the investigation discloses that the source of attack is a non-military U.S. citizen or that the
purpose of the attack is not related to national security, the investigation should promptly be placed under the control and direction of civilian law enforcement.

Even after relinquishing control to civilian law enforcement, military investigation of the incident for the purpose of preventing future attacks or for the purpose of patching vulnerabilities may lawfully continue, because prevention and vulnerability analysis on military computers are primarily military purposes.237 Further, to the extent that there remain military suspects, investigation of the involvement of those military suspects is proper. Once the FBI has control of the law enforcement investigation, however, it would be improper to interrogate civilian suspects or make other strategic “control” decisions that could substantially affect the civilian law-enforcement investigation, even if military suspects are involved.

In this resolution of the uncertainty problem it is important to note that resolution gives the military commander discretion to investigate the compromise of military systems. The resolution is not a command to investigate or to continue to investigate. The resources dedicated to repelling a particular attack and investigating its source and purpose are a matter of policy commended to the discretion and good judgment of the commander consistent with civilian oversight.

It is important to reiterate that this resolution relies upon the logic of Meeks’s reasoning as applied to the infrastructure protection uncertainty dilemma. In no way does this resolution depend upon the holding in O’Callahan, which has been overruled.

Civilian Witnesses in Military Investigations

In the process of tracking intrusions, military investigators will likely need to gather information from non-military personnel and systems. If the military purpose of an investigation is primary, military investigators may interact with civilians in the course of the investigation. Military police may administer a lie-detector test to a civilian witness, interrogate civilians (subject to their consent), give oaths to civilians in connection with such an investigation, and investigate DoD civilian employees.238 Therefore, military investigators can ask questions of system administrators at universities and private companies to gain information about an attack or intrusion, if those system administrators consent to the interview. Military investigators can gather copies of relevant private system logs and audit trails, subject to the consent of the private owner. Serving as primary investigators of a crime committed by a U.S. civilian is prohibited, however, notwithstanding the fact that resulting arrests would be made by law enforcement personnel.239 That prohibition follows directly from the uncertainty resolution analysis, above: When it appears that a U.S. civilian is the perpetrator of a crime, the matter is no longer primarily a national security concern and should be released to appropriate law enforcement agencies. Further, issuance and execution of search warrants and the exercise of subpoena power is probably best left to civilian law-enforcement authority, possibly a U.S. Attorney’s office, when the subject of the warrant or subpoena is the property or person of a civilian.240

Military Interest Computers

So far, this article has primarily discussed military response to attacks against military networks; however, the sphere of military interest encompasses many networks and computers owned by the federal government and privately owned companies. Federal government computers and networks collect and process intelligence data critical to military planning and
execution. Government and private networks carry the overwhelming majority of military communication. Commercial manufacturers of military weapons systems, information systems, and other goods consumed by the military possess classified and sensitive information. These civilian-owned computers and networks, some of which are expressly included in the Defense Information Infrastructure, are of legitimate interest to the military.

Government Computers
The President has the authority and power to protect federal property. Where federal property is in danger and local law enforcement authorities are unable to provide necessary protection, the President may order troops to protect such property. Federal troops have been properly used to guard the United States Mint, the residence and office of the United States High Commissioner to the Philippine Islands, the grave site of President Franklin D. Roosevelt, federal payrolls in the custody of the Post Office Department, and gold in transit on an emergency basis. Because this power is based upon inherent executive authority, and the justification of necessity, discussed above, the employment of military troops to protect federal assets should be limited in time to the period necessary, extending only until an adequate civilian force can be assembled.

Classified Contractors
There is a strong military purpose in protecting classified defense information. Regulation permits military personnel to gather information necessary to protect against compromise of classified defense contract information and protect against activities endangering facilities executing classified defense contracts. Such protection is proper under the military purpose exception.

Unclassified MilSpec Contractors
Courts have recognized a special relationship between the military services and those contractors that build products to military specification. Grounding itself on the uniquely federal interest in government procurement of equipment, the Supreme Court in Boyle v. United States extended (in a sense) sovereign immunity against defective product design to a commercial helicopter manufacturer. In that case, Boyle drowned when a military helicopter made a forced water landing. A defective design required by military specification prevented Boyle's escape from the passenger compartment, which proximately caused his death. Reasoning that one who is obligated to build pursuant to a government specification should not be liable for defective design when the government itself is immune, the Court found a conflict between state tort law, which imposed liability, and federal Constitutional law, which prevents such liability. As a result, the Court recognized a "military contractor defense" and held that the special relationship between military contractors and the government resulted in immunity for the contractor through preemption of state tort law, which would have otherwise held the contractor liable.

The Boyle Court set out a three-part test for the contractor to avoid liability: (1) reasonably precise government specifications, (2) contractor compliance with specifications, and (3) contractor warnings to the government regarding dangers known to the contractor but not the government. This is relevant because it establishes that not all contractors have a special relationship with government and it establishes a principle of "reasonably precise" government control to establish such a relationship.
The holding of Boyle does not speak precisely to the issue of the scope of military interest in contracted-for goods. Boyle is a preemption case, regarding the displacement of state law. In the context of the Posse Comitatus Act and military protection of civil infrastructures, there is no state law to displace, but the existence of a case like Boyle permits an inference that the military has a strong interest in the performance of reasonably precise milspec contracts. Further, if the military is to render assistance or require action of commercial, non-government entities regarding infrastructure protection, Boyle and the traditionally strong information-security relationship between the military services and milspec contractors make such contractors an obvious place to start.

If milspec contractors request assistance from the military services, military personnel can render assistance, provided the analyses under the Three Tests, the uncertainty problem resolution, and the military purpose exception are satisfied. Active participation is permitted if uncertainty about the identity and purpose of the attacker exist.

If security measures at milspec contractors were to become a concern, compliance with security standards could be incorporated into contract specifications and therefore into the performance duties of contractors. Contract solicitations could include inspection and audit clauses to permit military contracting or inspection personnel to ensure that information and networks were protected pursuant to the specification. Failure to comply could result in termination for default and recovery of reprocurement expenses and possibly other damages.

Commercial Off-the-Shelf Contractors

In the last several years, government contract reform has attempted to lower costs for commodity items by purchasing commercial off-the-shelf ("COTS") items under ordinary market terms using a simplified, streamlined acquisition process under Federal Acquisition Regulation part 15 ("FAR 15"). Many items, including major military weapons platforms, are built to milspec, but items that are mass produced for commercial markets are more efficiently procured in COTS acquisitions. Services may also be procured under COTS procedures.

The primary market driver for a COTS manufacturer is usually commercial demand, not military demand. For example, the market for personal computers to perform word processing and other office work is predominantly constructed to satisfy the non-military market for such products. The same is true of many other information technology products.

COTS contractors do not build to "reasonably precise" military specifications. They produce products to meet commercial demand, and military contracting officials purchase those products when they meet military needs. Therefore, under the Boyle test, courts would probably not afford COTS contractors an extension of sovereign immunity.

Failure to satisfy the Boyle test may break the special relationship recognized in Boyle; however, the uniquely federal interest in government procurement remains, at least in part. That uniquely federal interest may rest on the public interest protected by the government, and in particular the protective role of the military and the potential for tragic harm to the public interest from compromise of military operations. Therefore, even the attenuated connection between COTS contractors and military services may provide a basis for active investigation of threats to national security that arise from intrusions in COTS contractor networks.

One example of a legitimate military interest in protecting COTS contractor networks relates to vulnerabilities of COTS products. Much networking equipment purchased by mili-
tary services, including routers and hubs, is primarily produced for a commercial market. It is plausible that such routers may be purchased and installed at the base level in a FAR 15 acquisition. One threat to national security could arise if interests hostile to America infiltrated router manufacturer networks and accessed email or private listserv communications between engineers who were troubleshooting software and hardware failures. Some of the earliest, and probably most technically competent, descriptions of security vulnerabilities and how they may be exploited may occur in such supposedly private internal corporate communication. An intruder with access to such discussions could learn of a vulnerability in military (and other) routers and leverage that knowledge into access to military networks. Preventing such an occurrence would be a legitimate military interest, and if properly executed so the military purpose was primary, military personnel could investigate intrusions into COTS contractor networks. The uncertainty problem resolution and considerations discussed above regarding consent to interview civilian witnesses and the exercise of subpoena power apply in such investigations. Terms of the COTS contract may be written to provide necessary consent.

A potential national security concern may also arise through COTS acquisition of commercial services. Significant communication resources are controlled by milspec contract in the Defense Switched Network ("DSN") of leased lines; however, not all communication services consumed by military services are performed pursuant to milspec contract. Intruders have proven capable of controlling the public switched telephone network ("PSTN") to interfere with all calls to particular numbers, monitoring government wiretap activity, and compromising the privacy of PSTN communications. If such interference and monitoring were targeted at DSN communications, the milspec contractor special relationship rationale and legitimate military interest would justify tracking perpetrators and preventing future intrusions. Under a similar rationale, if the target were COTS-procured military communications on the PSTN, tracking and intrusion prevention would be legitimate military interests. Further, if there is a military impact, but it is unknown whether military communications are a target, the uncertainty problem resolution would apply to permit active military investigation at the request of, or with the consent of, the PSTN communications supplier.

Non-Contractor Networks
From the preceding analysis, it follows that a strong contractor-military link, like milspec compliance, brings intrusions more readily into the military sphere of interest. Where the contractor-military link is attenuated, a stronger tie between an intrusion and the military, such as a targeting of a military phone number on the PSTN, may be required to show a rational relationship between the intrusion and a legitimate military interest. From this sliding-scale model, it would appear that where there is no contractor-military link between a private company and a military service, there must be an exceedingly strong military interest to justify active military participation in defense of private infrastructure owned by non-contractors. This conclusion is confirmed by the telecommunications war powers of the President. In time of war, threat of war, or national emergency, the President may exercise varying amounts of control over wire and radio communications facilities. Emergency communications plans anticipate that the President will delegate some of the commandeered facilities under the control of the military for the purpose of defending the nation.
Summary

Consistent and proper operation of civilian-owned and operated communications networks is central to military command and control, and therefore a national security matter. Presidential directive mandates cooperation among defense, law enforcement, and intelligence agencies to protect critical national infrastructures. Military personnel may actively investigate, under the military purpose exception, when an unknown attacker with an unknown purpose is assaulting a military interest computer; however, if it becomes clear that the American civilian criminal courts are the proper forum for legal resolution of the matter, DoD must promptly transfer control of the investigation to an appropriate civilian law-enforcement agency. Continuing collateral investigation by military personnel is permitted if some military purpose remains, but such investigation should not interfere with the primary civilian investigation.

Part III: Application of the Act to Proposed Military Activity

With the Three Tests and the military purpose exception in mind, it is possible to meaningfully discuss contemplated military actions and whether the Act proscribes such actions. To restate the above discussed integration of the Three Tests: Prohibited activity is active, direct, partial (i.e., biased), or controlling of a suspect or investigation; conversely, permitted activity is passive, indirect, impartial (i.e., unbiased, without a stake in the outcome), and non-controlling.\textsuperscript{255} The Three Tests relate to active direct enforcement, pervasive activity, and use of regulatory, proscriptive, or compulsory power by military personnel.\textsuperscript{256}

Prevention, Preparation, Assessment, and Remediation

Preventive and Preparatory Activity in Military Interest Systems

In the infrastructure protection context, generally speaking, until an intrusion or attempted intrusion has occurred, no crime has been committed and there is no occasion to “execute the laws.”\textsuperscript{257} Preparation for cyber attack, strengthening of security precautions, and emergency planning with commercial information-service providers regarding use of diminished capacity and post-attack reconstitution are all proper activities and not prohibited executions of civilian laws.

The National Plan for infrastructure protection under continuing development by Presidential directive speaks of DoD analysis and assessment of vulnerabilities and remediation—“improv[ing] known deficiencies and weaknesses that could cause an outage or compromise a defense infrastructure sector or critical asset.”\textsuperscript{258} DoD actions as proposed in the National Plan are not necessarily limited to affecting DoD-owned or -controlled infrastructure assets; however, since no enforcement of law is occurring, such activities are permissible under the Three Tests. Even if laws were somehow being incidentally enforced, protecting defense infrastructure sectors and assets on the DoD critical assets list\textsuperscript{259} is a legitimate military interest, which would likely be the primary purpose of such military activity.

Finding and patching security holes in military systems and military interest systems is one ongoing preventive requirement. Preparing systems for anticipated attacks by erecting firewalls, installing access controls, and educating system users about good security practices is also
necessary. In addition, it may be desirable to implement intrusion tolerance measures. One intrusion tolerance measure is the use of encryption to protect communications and stored data, employed so that a breach of access control measures will not give an adversary access to clear text information. Even encrypting relatively unimportant data would slow an adversary down. Another intrusion tolerance measure is the classification and compartmentalization of information,260 and an accompanying set of layered access controls, employed so that a breach of security may be contained.

Such diagnoses of vulnerabilities, hardening of security measures, and preparation for attack are all permitted under the Three Tests. Planning, preparing, and coordinating with civilian organizations to improve civil defense and emergency preparedness are also outside the Act’s prohibitions.261 No attack (or crime) has occurred. There is no suspect or investigation to control. Nevertheless, when working with civilians not employed by DoD, military members should serve in an advisory role, never giving orders and always seeking consent for military activity that affects those civilians. Actively controlling such civilians may be an exercise of regulatory, proscriptive, or compulsory power in violation of the McArthur test.262 While giving orders would not constitute an execution of the civilian criminal laws, it could be construed to be enforcing some other laws or federal regulations that properly fall within the jurisdiction of another federal agency.

Expert Advice to Government and Civilians on Prevention and Preparation

Requests for military advice and recommendations regarding protection of systems that are not military interest systems may be honored. Advising government and civilian organizations in their preparations to protect such systems is permitted under the Act, because no offense has been committed. As in any context, advisors must be careful to recommend and not to command non-military personnel, because issuing orders could be subjecting civilians to military regulatory, compulsory, or proscriptive power in violation of the test in McArthur. Military participation on Interagency Expert Review Teams (“ERTs”), which plan information security measures and review plans composed by others,263 is proper, so long as military personnel participate in an advisory or commentative capacity.

Likewise, military advice regarding the application of intrusion detection techniques outside of DoD is proper under the Act. Presently, DoD possesses a technological lead over most federal agencies and commercial businesses in capacity for intrusion detection, especially as implemented over a geographically dispersed network containing hundreds of thousands of authorized users. The emerging plan for a Federal Intrusion Detection Network (FIDNET) to protect government computers may benefit from DoD expertise in building its own intrusion detection network,264 but military control over development of FIDNET in other government agencies would be an improper exercise of regulatory, compulsory, or proscriptive power. Advice and recommendations would be permitted.

Thwarting Attacks and Tracking Intruders

Intrusion Detection

The General Accounting Office estimates that DoD computers may have been subject to a quarter million attacks in 1995,265 however, reported figures during that period were much lower.266 Part of the difficulty in estimating the number of attacks results from a failure to detect attacks, and even intrusions, in progress. Developing early-warning systems and “net-
ted adaptive intrusion detection” measures may be a large part of DoD’s contribution to national infrastructure security. Such intrusion detection systems monitor system status and user commands to discover unusual activity. For example, performing a certain set of operating-system commands in sequence may be unusual for legitimate users, but characteristic of intruder attempts to gain privileged access. Noting such anomalous behavior and alerting system operators is an important part of defending infrastructures.

In the process of detecting intrusion, it is virtually certain that intrusion detection software, installed on DoD-owned computers and maintained by military personnel, will discover intrusions or attempted intrusions by civilians. At first, and perhaps forever, the identity of the attacker and the purpose of the attack will be unknown. As discussed above, applying the uncertainty dilemma resolution to these facts we see that repelling an unknown attacker is permitted under the military purpose exception to the Act. Further, investigating the intrusion to discover and remedy security vulnerabilities exploited by the attacker and to track the intrusion to its source are also permitted under that exception. If it reasonably appears that the proper forum for investigation and response is the civilian criminal courts, the FBI or another law enforcement agency must take control and direct the investigation. Until it reasonably appears that the proper forum is civilian, active, direct military participation is permitted. After that point indirect, passive assistance is permitted, if requested by the law enforcement agency controlling the investigation. In addition, after that point, military personnel should avoid interviewing civilian suspects, because such interviews could be considered controlling or directing an investigation where the proper forum is a civilian one.

To effectively detect unusual behavior, system administrators on military computers must install sniffers to monitor system activity. Such monitoring raises the general issue of privacy of legitimate users, but military organizations are required to post notices that use of communications and computer facilities constitutes consent to monitoring.

Participation in a larger effort to detect patterns of attack spanning many military, government, and possibly civilian sites is also proper, so long as military personnel are participating primarily to protect military interest computers or are participating passively at the request of law enforcement. For example, it has been proposed that DoD personnel work with private-sector industry leaders to share information with the FBI-run National Infrastructure Protection Center. Such activity would be proper. DoD personnel could share data uncovered in the ordinary course of duty while monitoring DoD networks and hand off investigations to NIPC as appropriate under the uncertainty problem resolution.

Discovery in the Ordinary Course of Duty

While performing intrusion detection functions and more generally, in the ordinary course of completing their duties, military personnel observe civilian criminal activity. Rather than forcing military personnel to turn a blind eye, the law permits such incriminating information to be handed off to law enforcement: “As a general rule, information obtained by military personnel in the course of performing military duties may lawfully be reported to civil authorities.”

In United States v. G. Hartley, Air Force inspectors discovered what they believed to be fraudulent tampering with military foodstuffs by a commercial supplier. Inspectors began to suspect that the samples of shrimp they had selected to test were switched with different samples before the testing could be completed. In a later delivery, the inspectors secretly marked the boxes of shrimp selected for testing. They did not consult with any criminal investigator or seek a search warrant before marking the boxes. When the marked samples
were removed and replaced with other boxes of shrimp before the testing process was complete, the inspectors requested that a criminal investigator be assigned to take over the investigation. Under the direction of a Defense Investigative Services civilian inspector, the marked boxes were located and used to incriminate the defendants.274

The defendants in G. Hartley moved to suppress evidence on the basis of a Posse Comitatus Act violation. In support of denial of the motion, on the issue of whether marking of the sample boxes by the inspectors constituted “execution of the laws by military personnel,” the court found “that this [marking] activity was undertaken on the initiative of the Air Force inspectors and was within the scope of their normal duties. The later revelation of their findings to the DIS was not in violation of the Posse Comitatus Act.”275

The G. Hartley court’s finding ties nicely with two concepts discussed in this article but not in the court’s opinion: first, that the marking of the boxes, which could be characterized as “active, direct and partial” could be permissible under the military purpose exception, to the extent that the ordinary course of duty equates with primary military purpose; second, that the reporting or “handoff” process was arguably passive assistance to law enforcement, and therefore not a violation of the Act. Such active ordinary-course discovery and passive handoff is a probable sequence of events for infrastructure attack investigations.

Meeks has commented on other situations where ordinary-course discovery followed by disclosure to law enforcement authorities would not violate the Act. Where military investigators acquire the names of civilian drug dealers from military sources and report the names to city law enforcement, there would be no violation.276 Where military pilots observe civilian criminal activity or the location of criminal civilian suspects incidental to their military flights and pass the information to law enforcement, there would be no violation.277 Military pilots and radar crews may report to the United States Customs Service regarding unidentified aircraft observed incidentally to military missions.278 Finally, federal statute permits the provision of information discovered “during the normal course of military operations” to law enforcement authorities.279

These findings and observations lend support to a military system administrator who, while monitoring a military interest computer network, browsing a webpage, or reading posts on a USENET listserver, discovers civilian criminal activity and passes the information on to civilian investigators. Note that the G. Hartley case appears to further reinforce a position that military personnel may, in the ordinary course of their duties, investigate to confirm a suspicion that something is amiss (e.g., swapped shrimp or compromised passwords) before reporting the matter to law enforcement.280

Search

Under Red Feather, search of an area for a civilian suspect is active, direct law enforcement.281 Active searching is permitted if a military purpose is primary, but not in assistance to an investigation with a primary civilian purpose. When requested by law enforcement, passive assistance using military personnel and equipment to monitor and communicate observations is permitted.282 Reporting on the relative position of law enforcement personnel and targeted criminal suspects may be permitted where it is impractical from a time or expense perspective for law enforcement personnel to procure and train to use equipment that permits the determination of a suspect’s position.283
Tracking and Investigation

Drawing upon and expanding the G. Hartley concept of investigating suspicious events to see if something is wrong, one may propose that military personnel track the source of a possible attack or intrusion. Applying the uncertainty problem resolution, tracking is certainly permitted, at least until it becomes apparent that the civilian criminal forum is appropriate. Nevertheless, even after the time when military investigators have ceded control of the investigation to the FBI or state and local authorities, military tracking may continue in at least two circumstances. First, relying on a Three Tests analysis, law enforcers may request passive assistance from military personnel in sorting through audit trails and understanding applicable technology. Second, military personnel on their own authority may continue to review intrusion detection log files, audit trails, sniffer log files, and other information in military possession to diagnose vulnerabilities exploited and implement a solution, even if that activity uncovers further incriminating information. If such incriminating information is incidentally uncovered, it must be passed on to civilian law enforcement.284

Notwithstanding this limited military authority to continue investigating, once law enforcement has control of the investigation, “strategic” decisions, like whether to interview witnesses or suspects, should be left to civilian law enforcement. If military members make such strategic decisions, there is a risk of violating the Act under the “pervasiveness” and “control” analyses in Jaramillo and McArthur.

Intrusion Research and Surveillance

Intrusion Techniques Research through Open Sources

To effectively counter threats of intrusion, military personnel must educate themselves about intrusion techniques. Intrusion technique tutorials, automated tools, and vulnerability information are available on public websites.285 Visiting such websites and analyzing publicly available resources are valuable opportunities to learn about vulnerabilities before an attacker exploits them. Such activity is similar to other vulnerability research, discussed above. There is no crime, and no suspect; therefore, there is no violation of the Act under the Three Tests.

A more difficult analysis is required if the gathering of vulnerability information is to be accomplished by infiltrating computer underground groups. In this context, there are two important points of distinction. First, it is important to distinguish listening from talking. Second, the gathering of vulnerability information is different from the gathering of information about those who have exploited (or might exploit) those vulnerabilities.

On the first point, if a group of persons is talking in a public forum, for example in a USENET group like <alt.hackers.malicious> or <alt.2600>,286 military personnel may simply read what those persons publicly post, by arguing that such “listening” is akin to viewing publicly available websites. Arguably, there is no crime or suspect, and so no violation of the Act. If criminal activity is discovered in this listening process, the listening is arguably passive, not directed at any person or objective (it is indirect and impartial) and not controlling of any person who could be a suspect. Under the Three Tests, then, such military listening activity is not prohibited. Information on civilian criminal activity should be passed to civilian authorities.

If, however, a military member speaks in such a public forum where criminal activity is suspected, perhaps in the hope of getting a focused response, the conduct has become more
active and direct and may fail the Three Tests, particularly the Red Feather test. This is especially true if the member is using a pseudonym, which could be considered an attempt to operate undercover. In soliciting a possibly incriminating response, the holding of United States v. Walden may apply. In Walden, Marine Corps personnel acted as undercover operatives and solicited incriminating responses from civilian suspects. In so doing, they became “principal investigators of a civilian crime” in violation of the regulations based upon the prohibitions of the Act. It may be argued that the military purpose exception applies when it is uncertain whether discussion participants are American civilians; however, military personnel who would act in such an undercover fashion should be prepared to show that reasonable precautions were taken to prevent incriminating responses by American civilians and that such a response was unlikely. Demonstrating precautions that could be expected to be effective may be difficult when the discussion occurs in a public forum like a USenet group.

On the second point, even where no criminal activity is suspected, collection of information through public sources about American civilians who may later become involved in criminal activity relevant to military interests is generally disfavored. A controversy regarding such “spying on Americans” by the military was resolved by the Supreme Court in favor of the Army on technical grounds in Laird v. Tatum, but the Court noted specifically that it was not sanctioning such information collection. The distinction here is between gathering information about vulnerabilities from public sources (permissible) and gathering information about American citizens from public sources to build a database of potential offenders (probably impermissible). It is advisable when harvesting vulnerability information from public sources to take precautions against creating records that attribute any information gathered to an American civilian or a person that could reasonably be an American civilian.

In any event, if information gathering turns up activity that may be related to national security concerns, the uncertainty dilemma resolution analysis should be applied to ensure that handoff to the FBI or other law enforcement agency occurs in a timely manner if it becomes apparent that the civilian criminal court system has become the appropriate forum for investigation and prosecution.

Surveillance

The distinction drawn above between gathering information from open sources and gathering information by actively participating in discussion applies equally to surveillance. Surveillance of places—for example, by employing sniffers on military interest computers or installing security cameras on military property—is permissible because it is passive. Such “place” surveillance would generally require the consent of the system owner (or a court order), and possibly the consent of legitimate users. Place-oriented sniffers should target types of activity and not particular persons.

Surveillance of particular people, in sharp contrast, is targeted, active investigation. Where American civilians are the targets of surveillance because they may perpetrate bad acts, military personnel encounter the almost-admonition of Laird and DoD policy counseling against spying on Americans. Specifically, DoD policy prohibits collecting, processing, or storing information on non-DoD individuals or organizations, except where essential to protect DoD functions or property, ensure personnel security, and deal with civil disturbances. Where American civilians have committed crimes, handoff to law enforcement is appropriate. Surveillance may discover a particular intruder, identified as an American civilian,
making repeated unauthorized entries into military or military interest computers. In that case, military personnel may log the intruder’s activity to discover vulnerabilities and remedy them, but should pass such logs on to the controlling civilian law-enforcement agency to passively assist in the law enforcement investigation.

Some guidance can be found in administrative determinations focused on aerial surveillance. In those administrative decisions, the Judge Advocate General of the Air Force ("TJAG") determined that “aerial reconnaissance missions in support of civilian [law enforcement agencies] [were] intended for . . . the reconnaissance of property and not for the surveillance of persons.” TJAG also drew a “distinction between actions directed at persons versus those directed at property” and closely linked that distinction to concurrence with an assessment “that Congress did not intend to prohibit all forms of surveillance.” TJAG’s opinions addressed aerial reconnaissance in the context of title 10 United States Code section 374, but, as discussed above, section 374 and its companion statutes were generally clarification statutes, not expansions of authority; therefore, section 374 and TJAG’s opinions may also apply to infrastructure-protection-related surveillance.

Coordination of Research and Development

The National Plan describes a program to establish “University Centers of Excellence” to promote development of cyber security as a course of study and instruction among graduate and undergraduate students. The Plan proposes DoD and the National Security Agency as two agencies that may be best equipped to manage such a program. Such oversight would be proper if DoD control were contemplated in the appropriations legislation for the program, because any extension of regulatory or law enforcement power by act of Congress is a statutory exception to the Act. Coordination or management of other university research relating to information security and other matters of concern to DoD is also proper if applicable appropriations legislation is passed.

Attacks on Non-Military Networks

Material regarding attacks on non-military networks is distributed throughout this article. This section focuses on attacks against civilian networks in which the military has no particular interest, except in its mission to protect the lives and safety of Americans and the well-being and prosperity of the nation. Discussions of permissible activity relating to civilian-owned and -operated military interest computers and critical defense information infrastructure assets are incorporated into analyses that discuss military and military interest computers in this Part III. Military purpose ties to the protection of military contractor and other civilian networks and computers is discussed above in the Military Interest Computers section of Part II.

Expert Advice during Attack on Civilian or Non-Defense Government Networks

Expert advice is passive assistance as defined by McArthur and Red Feather. If civilian authorities or private civilian organizations request military assistance, including “tactical” advice on subjects including repelling attacks, expelling intruders, preserving audit trails for tracking, “triage,” protection of key resources, and reconstitution, such assistance is proper under the Act.

If there is no primary military purpose for active participation, such as an attack on military interest computers from an unknown source, active participation by military members...
Pressing keys on a keyboard with the objective of accomplishing any of the above tactical actions would likely be considered active participation under Red Feather. Directing or controlling defensive activity would likely be considered impermissibly pervasive under Jaramillo or compulsory under McArthur.

The National Plan proposes integration of DoD and intelligence community analysts into the NIPC. Such analysts would participate in an integrated analysis and defense of military, government, and private systems. Active participation of military NIPC analysts would be proper under the following circumstances: first, if the use of DoD personnel is permitted under applicable legislation passed to effect proposals of the National Plan; second, if the use of DoD analysts is temporary, until sufficient civilian expertise develops, and third, if the DoD analysts primarily pursue legitimate military interests. Legitimate military interests include analyzing threats to military networks and military interest computers using the assets and information available to NIPC, acting as an information-sharing liaison between the military services and the NIPC, and facilitating military response to attacks in progress against military interest computers detected by NIPC. Passive participation would be proper if the military analyst was in a purely advisory role.

Preparation to Use Military Forces during Attack on Civilian Networks
When military emergency preparation requires operation in an environment where violations of law are occurring, a commander may rely upon McArthur to establish that pre-emergency planning is a legitimate military interest. Of course, there must be a reasonable likelihood that military assistance will be required, and permitted under an applicable emergency exception, to permit such “on-scene” preparations. In McArthur, for example, there was a reasonable likelihood that military force could have been used to suppress insurrection at Wounded Knee, South Dakota. The court commented of two Army colonels on scene,

Colonel Warner and Colonel Potter had another principal duty, that of being prepared to “use a part of the Army or Air Force to execute the laws” if the President should determine that was necessary. This preparation for a possible future military act by responsible military men cannot be equated to the actual use by civilian authorities of a part of the Army or Air Force to execute the laws.

Therefore, if a series of intrusions of civilian sites with no military connection appeared reasonably likely to precipitate a civil defense emergency, the military could prepare to assist civilian network operators, even before an emergency was declared. Such a situation could occur if widespread attacks against telecommunications service providers or electric power distribution infrastructure began to threaten the operation of emergency services (fire, medical, police) or endanger civilian lives. Such preparations would be proper, even if it could be definitively established that the source of the attacks was domestic. Execution of an emergency plan by military personnel in such a situation would be proper only after an emergency was declared by the President, or once the threat to life became so imminent that it justified timely intervention by local commanders acting independently.
Military Mitigation of Emergency

If the President declares an emergency and orders military members to assist in reconstitution after a catastrophic regional or national infrastructure collapse or to mitigate or contain damage or loss of life from such an event, active or passive assistance, as ordered, is proper under the emergency exception. Emergency response by local commanders may also be justified to save lives or prevent wanton property damage, but commanders should seek guidance from their superiors immediately regarding continued activity, before ordering military action, if possible.

Public Education

Offering DoD infrastructure protection knowledge to government and industry increases national preparedness for infrastructure attack. Teaching materials and personal instruction by military members do not violate the Act. One example of such efforts already under way is the creation by the DoD Infosec program of a series of seventeen CD-ROMs and videos for use throughout the federal government.

Protecting Good Order and Discipline

Commanders possess inherent authority to maintain good order and discipline on military installations, but a commander should be careful when relying upon maintenance of good order and discipline as a primary military purpose to justify active participation in civil law enforcement activities. Almost anything with a peripheral or incidental relation to any military service can be connected to good order and discipline. In Walden, for example, Marine Corps advocates could have argued that benefits to good order and discipline—preventing the introduction of illegally purchased weapons on base—justified an undercover gun buy to ensure that sellers complied with state residency and age requirements. Such a connection between an undercover enforcement operation and Marines, who could possibly be out-of-state or underage purchasers, would likely have been insufficient to justify Marine troops acting as undercover agents in the sting operation. The primary military purpose exception discards incidental connections to good order and discipline, such as the possibility that military-related infractions will occur, as insufficient to permit active law enforcement. Fundamentally, good order and discipline decisions are balancing tests.

One good model to evaluate the strength of a good order and discipline military interest in law enforcement activity is the Memo 5 Operation. Memo 5 Operations may be conducted by, for example, the Air Force Office of Special Investigation in conjunction with local law enforcement officials to stem a flow of illegal drugs to military members from the civilian community surrounding a military installation. Ready availability of illegal drugs to troops interferes with the maintenance of good order and discipline on base, in a manner comparatively more serious than the possession of lawfully manufactured guns in Walden when such guns were purchased in technical violation of gun-retailing laws. In such drug cases, reliable information points to a civilian source of supply outside the jurisdiction of AFOSI special agents. Often, a military member with a connection to the civilian drug dealer will volunteer to gather evidence. AFOSI agents may propose a controlled buy, where the military member uses marked bills to purchase drugs and agrees to testify against the dealer. Civilian law enforcement controls the operation, makes arrests, and handles involved civilians.
While such participation would appear on its face to violate the Act, such conduct can be justified as primarily military in purpose if the evidence strongly connects military member drug use and the existence of drugs on base to the targeted civilian source of supply. Justifications are carefully thought through, prepared in writing, coordinated with the Staff Judge Advocate’s office, and forwarded to higher headquarters for analysis and decision whether to permit the proposed operation. In situations where it is not obvious whether a desired information infrastructure protection operation is permissible under the Act, following a procedure analogous to the Memo 5 procedure may help make an informed, prudent decision.

Military Operations: Defensive Strikeback

Strikeback falls into a category separate from others so far discussed. Strikeback is an in-kind retaliation to incapacitate an intruder. One example was DoD’s April 1998 browser crash strikeback against a denial-of-service attack by the Electronic Disturbance Theater (“EDT”). EDT attack participants sent rapid and repeated requests for information to DoD webservers. DoD system administrators diagnosed the form of attack, discovered how to screen attackers from legitimate requests, and flooded attackers’ computers with open-window commands, which eventually caused the computers of some attackers to crash.

While an exceedingly weak argument exists that strikeback may constitute “punishment” without due process of law, such in-kind retaliation is a military operation conceptually different from law enforcement. The punishment argument may have more merit when the targets of strikeback are American civilians, but to the extent that strikeback is focused on expelling intruders and precluding continuing attack, strikeback more closely resembles self-defense than punishment. Self-defense is a justification of necessity. In the case of the EDT strikeback, the browser counterattack was a method to expel attackers and stop a malicious interference with services.

Some legal danger may arise if a strikeback is erroneously targeted. If an intruder is unlawfully using a third-party computer to launch the attack, that third party may complain or even seek damages in tort for damage caused in a strikeback. A factual defense to such a lawsuit, arguing that the strikeback was a “reasonable” response under the circumstances, may succeed. If it does not succeed, a contributory negligence defense might prove unsuccessful because strikeback actions are intentional; however, a possible counterclaim could be mounted that the third party negligently operated or negligently “entrusted” the computer system used in the attack.

To the extent that in-kind retaliation is necessary self-defense, it is not law enforcement, and so is not prohibited by the Act. This necessity justification has yet to be tested by the courts in the computer network context, however. In any event, other legal dangers counsel against use of a strikeback capacity without careful consideration, especially if the strike would be expected to cause more damage than a system crash and non-damaging restart. Further, public confidence in military infrastructure defenders could suffer if counterattacks were erroneously targeted.
Prohibited Activity

Search, Seizure, Arrest, and Prosecution

Arrest, interrogation, and prosecution of civilian suspects are matters for civilian criminal law enforcement agencies. Searches and seizures of civilian property are properly conducted by civilian law-enforcement officials. Consent, or an invitation, from a witness to search through evidence or take evidence or copies of evidence relevant to a primary-purpose military investigation makes such “search” and “seizure” permissible, but military personnel should not interrogate or arrest a civilian suspect or search or seize the property of a civilian suspect. Even in primary-purpose military investigations, military commanders should ensure that their legal advisors approach the U.S. Attorney’s Office or the FBI for assistance in non-consensual searches or seizures of civilian property. Determining punishment for convicted civilians is the province of the civilian criminal courts. Notwithstanding the above, arrest, interrogation, prosecution, and punishment of military members by military members is expressly permitted by the Uniform Code of Military Justice, which serves an exception to the Act permitting these actions against persons subject to the Code.

Criminal at-Large/Escaped Prisoner

When a criminal poses a general threat to the military community, but is properly the subject of action by the civilian criminal court or penal system, military personnel may not actively participate in bringing the criminal under control. For example, in Wrynn v. United States when Air Force pilots used a military helicopter to pursue an escaped civilian prisoner near a military base, the court found a violation of the Act. The Wrynn court contrasted the pilots’ activity with the lawful actions of a commander of ground troops, who disbanded and disarmed the military search party under his control when he learned that the escaped prisoner was not a military member. In the process of procuring resources needed to facilitate escape, the prisoner could have harmed troops or their families living on or near the military base. Consequently, a threat to the military community existed, but because the prisoner had escaped from a civilian facility and had no connection to the military, the search-and-apprehend activity was primarily a law enforcement activity and only incidentally a military one. This situation can be extended to the infrastructure protection context: Where an intruder is trespassing in military and civilian systems, and has been identified as a civilian, but is evading capture, tracking and apprehension of the intruder is primarily a law enforcement operation and not primarily military. Therefore, military personnel may passively assist in a civilian-controlled investigation and may actively investigate with the primary purpose of securing military systems against further intrusion, but may not actively participate in law enforcement and tracking, even though the intruder at-large could cause harm to military systems.

Summary

Generally speaking, preventive and preparatory activity to protect military interest computers is permissible under the Act. Tracking intruders is proper only if the military purpose for tracking is primarily a military one. Research on intrusion through open sources is proper, but DoD should not gather information about particular persons when performing such research. Coordination of government expenditure of research funds is permitted with con-
gressional approval. The Act permits surveillance of places, but not people. Military personnel may investigate intrusions into civilian-owned networks where the military purpose is primary and with consent of the network owners. Defensive in-kind strikeback against attackers by military information operators may be justified by necessity, but numerous legal and policy dangers should be considered before engaging military personnel in such activity. Search, seizure, arrest, and prosecution of civilians by military personnel is generally prohibited.

Part IV: Recommendations for Officials

The Conservative View

Situations where commanders and other officials are in danger of violating the Act’s prohibitions center on military interactions with civilians when a civilian has committed a crime. While it is permissible for military members to continue some independent investigation, as discussed above, after learning that a crime’s likely perpetrator is an American civilian a conservative commander would cede control of the investigation immediately to civilian law-enforcement officials. Permitting civilian law-enforcement investigators to determine how and when to gather evidence, including whether and when to interview particular military or civilian witnesses and perhaps even when and how to interrogate any military suspects wrapped up in the civilian-related crime, will keep the commander out of trouble. The commander can assist the civilian investigation by making available military personnel, records, equipment, and expertise as requested by law enforcement and by volunteering information discovered by military system administrators and network workers in the ordinary course of duty. This kind of assistance and coordination is expressly contemplated by PDD 63, and is appropriate and proper and not a violation of the Act.

Further, preparatory actions, which are not focused upon investigating a particular intrusion, are not violations of the Act. Commanders may direct military members to install intrusion detection systems, audit trail software, and sniffers in military networks and in military interest civilian networks where consent has been procured. Commanders may direct military members to search for and patch system vulnerabilities. Commanders may originate programs that configure networks in a manner that will facilitate tracking and identification of intruders when attacks occur. Commanders may share such information and expertise in intrusion detection, tolerance, and tracking with other government agencies and with civilian infrastructure owners and operators.327

This conservative view avoids all reasonably probable conflict with the Act. It permits preparatory actions and hardening of network systems, gathering of intrusion information in the ordinary course of maintaining network systems, responding to attacks and intrusions from unknown sources and national security threat sources, and passive assistance to law enforcement officials in their investigations of civilian crimes.
Policy

Once an analysis applies the prohibitions of the Act to a proposed action and determines that the action is within the discretion of the commander, the commander should consider other factors including military readiness, public response, and likely effectiveness of the action to accomplish the stated objective. One important factor that affects all of these matters is training.

Operational Readiness

Soldiers are taught to respond to an ambush with immediate suppressing fire and then maneuver, if possible. At the squad level, an immediate response with maximum available firepower provides the best chance of survival in an ambush. Delay is literally fatal. Activities that dull the warfighting response or detract from training a soldier to take and hold land may adversely affect operational readiness. On the other hand, many military members perform specialized computer-related tasks more closely akin to protecting electronic communications and networks than to taking and holding ground. For those troops, readiness may actually benefit from a real-world training opportunity to assist infrastructure protection efforts.

The broad range of civilian infrastructure protection actions within commander discretion permits the commitment of staggering resources to activities with possibly peripheral military utility. Budget and personnel constraints require that limits be set on military assistance to civilian organizations. Congress has recognized the need to relieve the military of the burden of assisting civilian organizations if such assistance would impact military readiness. If readiness would be compromised by diverting military resources to assist civilian infrastructure efforts, commanders may exercise their discretion to deny a request for assistance; however, that denial should be made on policy grounds and not on the basis of the Posse Comitatus Act, unless the Act really applies.

Public Response

A second policy matter for commanders to consider is public response. The Laird Court noted the public’s “traditional and strong resistance...to any military intrusion into civilian affairs.” Indeed, in the facts leading to the filing of suit in Laird, the public viewed military collection of information about those who might incite or become involved in an insurrection as “spying on Americans.” Defense policy today, embodied in regulation, prevents real-time electronic eavesdropping by DoD personnel and real-time translation of conversations between American citizens. Public support is important. Decisions and policies should consider the impact of public sentiment.

Appropriate to their mission, civilian law-enforcement personnel are trained to deal with Miranda warnings, the application of non-lethal force to subdue dangerous persons, and the (hopefully rare) application of lethal force when police officers or others are threatened with death or serious bodily injury at the hands of a dangerous person. In sharp contrast, military personnel are trained to precisely apply lethal force on a large scale, usually with a goal of achieving dominance in a relevant “battlespace.” Military personnel are not generally trained to protect Constitutional rights, in part because their primary mission will usually not bring their actions into conflict with the Constitutional rights of Americans or protected persons on American soil. Training received is generally not appropriate for either group to accomplish tasks better suited for the other. One can imagine that well-trained law enforcement personnel may make many deadly mistakes on a military battlefield. Like-
wise, military personnel may make many Constitutionally prohibited or physically fatal mistakes in a law enforcement context. While it is unlikely that police would find themselves on a traditional battlefield, infrastructure protection by DoD will expose some soldiers to law enforcement issues every day. The likelihood and consequences of a possible mistake should receive a commander’s express consideration. Experience has shown that press coverage can also amplify public response.337

Accomplishment of the Stated Objective

A third policy consideration flows directly from the different training required to accomplish law enforcement tasks and military tasks. Some military personnel may simply be ineffective at accomplishing some law enforcement tasks. They may not have received the training necessary to complete such tasks without making important mistakes. A commander should therefore consider whether the commitment of military resources will have a positive effect that outweighs the cost of committing them.

Defenses

Against Criminal Liability

The Act prohibits “willful[ ] use[ of] . . . the Army or the Air Force . . . to execute the laws. . . .”338 A willful act is deliberate and done with the specific intent to do something that the law forbids.339 A willful actor intends the result that comes to pass.340 The Act is a criminal statute. In the criminal context, a requirement that an offense be committed willfully is satisfied if a person acts knowingly with respect to the material elements of the offense.341

Good faith is opposite in intent from willful commission of an offense. “In common usage [good faith] is used to describe that state of mind denoting honesty of purpose, freedom from intention to defraud, and, generally speaking, means being faithful to one’s duty or obligation.”342 In less formal parlance, good faith by a military commander can be taken to mean a genuine belief by the commander that he or she is pursuing a legitimate military objective, and a genuine belief by the commander that the method used to accomplish that objective is allowed under law.

O’Shaughnessy has suggested that a commander who has acted in good faith but is charged with a violation of the Act might defend on the basis of lack of specific intent.343 No prosecutions of military personnel for violations of the Act have occurred, and therefore the good-faith defense has not been tested. O’Shaughnessy’s view gains some support from Walden, where the court considered that government employees had acted without intent: “[T]here is totally lacking any evidence that there was a conscious, deliberate or willful intent on the part of the Marines or the Treasury Department’s Special Investigators to violate the Instruction or the spirit of the Posse Comitatus Act.”344 The court in Walden discusses the “Instruction” and the “spirit” of the Act, and not the Act itself, because the military personnel found to be actively participating in law enforcement activity were Marines—Department of Navy personnel who are not covered by the Act’s prohibitions, but instead are covered by Navy regulation that mirrors the Act. Further, the trial was one against the defendant charged with violating federal firearms laws, whom the Marines were investigating, not against the Marines or the Treasury Agents for violation of the Act.
Intent to break the law is usually less relevant than the purpose to cause a prohibited series of events to occur. Therefore if a person, ignorant of a legal prohibition, intends to cause an event that is sanctioned by criminal law and actually causes that event, a willfulness requirement in that legal prohibition generally will be satisfied.

The meaning of the word willful depends in large measure upon the nature of the criminal act and the facts of the particular case. It is only in very few criminal cases that willful means done with a bad purpose. Generally, it means no more than that the person charged with the duty knows what he is doing. It does not mean that in addition he must suppose that he is breaking the law.345

While this language would provide a strong argument against a good-faith defense, it does expressly recognize that the meaning of willful depends upon the nature of the criminal act charged and the facts of the case.

An analogy can be drawn between a commander attempting in good faith to discharge duties in compliance with the Act and a police officer attempting in good faith to discharge duties while executing a search warrant. A police officer may willfully enter a person’s home in reliance on a search warrant. If that search warrant is invalid for a reason that is not within the knowledge of the officer, the officer would not be charged with breaking and entering or trespass. Likewise, a commander may intend to act as a principal investigator of a crime and may not know that such activity, in the particular context, violates the Act. If the officer knows of and intends to comply with criminal laws relating to housebreaking and trespass, good faith protects the officer. Likewise, if the commander, another government servant, knows of the Act and intends to comply with the Act, good faith should also protect the commander. The common elements of government service, knowledge of relevant law and good-faith intent to comply, argue strongly for a contextual good-faith defense. The Walden court’s discussion of good faith further supports this contextual interpretation of criminal willfulness.

When deciding upon a course of action, commander solicitation of and adherence to advice and opinion of legal counsel would provide helpful evidence that the commander specifically intended to comply with the Act’s prohibitions. Counsel should look at recent developments but may rely upon scholarly writings, as modified by recent cases, legislation, or regulation. If time permits, counsel should prepare a written opinion addressed to the commander.

Against Civil Liability

If violation of the Act breaks the bonds of agency with the government, and a government official is exposed to personal civil liability in a suit charging violation of a Constitutional right, a defense may be mounted upon Harlow v. Fitzgerald.346 Under Harlow, a government official who violates a Constitutional right that was not “clearly established” at the time of the violation is immune from civil liability. This immunity may attach even if the official acts with knowledge that the action is unconstitutional.347

As discussed above, courts have not clearly established a personal Constitutional right to be free from military involvement in civilian law enforcement. Without a clearly established right, an official is immune for Constitutional claims arising from violation of the Act.

The Harlow decision also precludes liability for statutory claims that are not “clearly established.”350 It is an open question whether the Act clearly establishes a personal right to recover in tort against an official, or whether the claim is novel. Considering that damages
have not yet been awarded for a violation of the Act, it may be possible to defend using Harlow.

A counterargument to the Harlow defense may be found in Lamont v. Haig. While discussing the Act, the Lamont court stated “that members of the military, like other public officials, are subject to suit for the individual commission of common-law torts.” A plaintiff could rely on that statement to help demonstrate clear establishment of a statutory right under the Act.

Summary

In determining whether to commence an investigation related to a network attack, commanders should consider the impact on operational readiness, projected public response, and fitness of military troops for accomplishing the given task. If, after reviewing such policy matters, a commander orders that a military investigation begin, the greatest danger of violating the Act arises when military personnel interact with civilian witnesses or a civilian suspect after learning that a civilian is responsible for the intrusion. Upon learning that a crime’s likely perpetrator is an American civilian, a conservative commander would immediately transfer control of any investigation to civilian law-enforcement officials. Liability for financial damages and criminal prosecution of violators of the Act are possible but extremely unlikely if the violator acts in good faith; nevertheless, a commander should seek legal advice before committing military troops to law enforcement matters if at all possible.

Part V: Conclusion

Action by military commanders in support of national infrastructure protection efforts is somewhat restricted by the Posse Comitatus Act, which prohibits the active direct enforcement of civilian laws by military members. Discretion of those commanders, however, is much broader than popularly conceived. In general, passive military assistance to law enforcement is permitted where such activity is indirect, not partial, and non-controlling. Even if military activity is active, pervasive, direct, controlling, compulsory, proscriptive, or regulatory with respect to civilians, such activity may be permitted under a military purpose exception, an emergency exception, or any of several statutory exceptions enacted by Congress.

By applying the analyses set out in this article, commanders can more accurately understand the scope of discretion afforded them by the Act. Such an understanding would permit commanders to decide on the basis of policy whether a contemplated action is proper, and not dismiss the action as impermissible because of an overly broad conception of the Act’s prohibitions.

It is hoped that this description of the Act’s prohibitions may assist Congress to define the desirable scope of commander discretion. The statutory exceptions for biological, chemical, and nuclear threats indicate that where weapons threaten the lives of many Americans, Congress is willing to create an exception to the Act. If information-warfare technologies and American dependence on information infrastructures develop to a point where IW attacks may kill thousands or cause vast economic harm, Congress may choose to pass a statutory exception regarding protection of information infrastructures. Such an IW threat seems more
credible in light of the comments of the President, a former secretary of defense and a former director of the CIA, who place information-warfare threats alongside chemical, biological, and nuclear threats. In the interim, the analyses in this article may assist commanders in deciding how to address such threats.

Notes


4 PDD 63 at 2 (“no later than five years from the day the President signed [PDD 63 (May 22, 1998)] the United States shall have achieved and shall maintain the ability to protect our nation's critical national infrastructures. . . .”); id. at 6 (“the Principals Committee should submit to the President a schedule for completion of the National Infrastructure Assurance Plan. . . .”).


7 PCCIP Report, supra, note 1 at 3–4.

8 See id. at 3–6.

9 See id. at 14.


11 Id. at xiii.

12 Alderson, supra, note 3 at 1 (summarizing remarks of General Tom Marsh, USAF (Ret.), Chairman of the PCCIP).


14 Interview with Richard Hafner, Product Line Manager, Information Systems and Telecommunications, EPRI; Rambabu Adapa, Product Line Leader, Transmission Substations
and Grid Operations, EPRI; and Massoud Amin, Manager, Energy Delivery and Utilization, EPRI, in Palo Alto, Calif. (Mar. 2, 1999).


16 Id.


19 See, e.g., 47 C.F.R. pt. 216, App., 775-76, ¶ 16.c. (1998) (placing national security leadership priorities above civil defense priorities); 47 C.F.R. § 211.5 (placing some civil defense activities at an equal level of priority with some military activities).

20 See, infra, notes 174-189 and accompanying text.

21 Military input to emergency plans has already occurred and should properly continue. See, e.g., 47 C.F.R. pt. 216, App. (describing allocations of resources based on military and civilian needs); id. § 202.2.


25 Id. But see, e.g., Cal. Penal Code § 150 (Deering Supp. 1999) (establishing a more modern obligation for all “able-bodied person[s] above 18 years”).


27 18 U.S.C. § 1385 (Supp. 1999). See also, supra, note 22 (citing the Act as first passed in 1878).

28 See, infra, notes 54-58 and accompanying text.

29 See Note, Honored in the Breech: Presidential Authority to Execute the Laws with Military Force, 83 Yale L.J. 130, 142-43 (1973) [hereinafter Honored in the Breech]; Furman at 93-95 (“This outrageous meddling in [the 1876 Presidential] elections was the moving case
of the Posse Comitatus Act's proposal and passage.

30 See Furman at 92–96; O'Shaughnessy at 704–05.

31 Paul Jackson Rice, New Laws And Insights Encircle The Posse Comitatus Act, 104 M I L. L. REV. 109, 112 (1984) [hereinafter Rice]. See also, M eeks at 97 ("[M]embers of a dissident Indian group forcibly took control of the village of Wounded Knee, held hostages, entered the U.S. Post Office by force, established an armed perimeter and denied federal investigators access to the area. . . .").

32 See generally, Rice (discussing the statutes).

33 See generally, id.; O'Shaughnessy; Furman; Honored in the Breech; M eeks; Siemer & Effron.


36 Chandler v. United States, 171 F.2d 921, 936 (1 Cir. 1948), cert. denied, 336 U.S. 918 (1949).

37 See also, O’Shaughnessy, supra, note 26 at 717, n.76.

38 E.g., United States v. Hartley, 796 F. 2d 112, 115 (5 Cir. 1986) ("If this Court should be confronted in the future with widespread and repeated violations of the Posse Comitatus Act an exclusionary rule can be fashioned at that time." (quoting United States v. Wolffs, 594 F.2d 77, 85 (5 Cir. 1979) (internal quotation marks omitted))). But see Taylor v. State, P.2d 522, 525 (Okl. Crim. App. 1982) (excluding evidence acquired in violation of the Act because of excessive, “intolerable” military intervention); Hawaii v. Pattioay, 896 P.2d 911, 925 (Haw. 1995) (excluding evidence acquired in violation of the Act “to vindicate the court’s authority”). Scholarly analysis comparing the Pattioay decision to decisions in other jurisdictions has suggested that the Hawaii Supreme Court may have overreached in finding a violation and in applying an exclusionary rule. See Jonathan W. Hitesman, Note, Fighting in Another Direction: The Posse Comitatus Act and the War on Drugs in Hawaii under State v. Pattioay, 18 Hawaii. L.Rev. 835, 849-864 (1996).

39 See, e.g., Furman, supra, note 26 at 86; Rice, supra, note 31 at 109; O’Shaughnessy at 723, 28–29.

40 The view that interpretation of the Act has in practice been “unnecessarily restrictive” is not new. See Furman at 128.

The pattern of interpretation of the Act has, in the author’s opinion, been unnecessarily restrictive. By using the Act as an excuse, the Army has succeeded in avoiding many time-, man- and equipment-consuming tasks. Doubtless, some of the proposed mis-
sions would have greatly detracted from the mission of national defense but they should have been rejected as a matter of policy and not of law, for many of the negative answers to queries on the use of the Army are legally unsound. . . . Id.


41 Indeed, the oath of office requires the military officer to support and defend the Constitution, which sets forth the mechanism for selecting civilian authority and limits the power of the military through civilian control. See, e.g., Air Force Instruction 36-2501, Officer Promotions and Selective Continuation, atch. 4 (Mar. 6, 1998) [hereinafter AFI 36-2501]. However, while military members are permitted to vote, regulation forbids participation in partisan political management, campaigns or conventions, publication of partisan political writings, and the making of campaign contributions to federal employees. Donald J. Atwood, Dep’t of Defense Directive 1344.10, Political Activities by Members of the Armed Forces on Active Duty, ¶¶ D.1.a., D.1.b.(3)-(4) and encl. 3 ¶ C.6. (June 15, 1990). This separation is further illustrated by the general prohibition on serving simultaneously as a military officer and an elected official. Id. ¶¶ D.1.b.(2), D.2., D.3.

42 See 10 U.S.C. § 151 (1998) (specifying the Joint Chiefs of Staff as advisors to the Executive Branch and permitting the Joint Chiefs to address Congress).

43 419 F. Supp. 186, 195 (D.N.D. 1975), aff’d sub nom. United States v. Casper, 541 F.2d 1275 (8 Cir. 1976), cert. denied, 430 U.S. 970 (1977) (recognizing that the expert tactical advice of a Colonel Warner was of “immeasurable value” to civilian law enforcement in the unrest at Wounded Knee).

44 Hammond, supra, note 34 at 961. In fact, one scholar has commented that “[t]he variety of interpretations [the Act] has received suggest [it] is so vague and indefinite that, as a criminal statute, it might be unconstitutional.” Furman at 86. It may be important to note that Furman made the comment in 1960 before Congress passed clarifying statutes in 1981.

45 See, e.g., Wryn v. United States, 200 F. Supp. 457, 465 (E.D.N.Y. 1961) (denying recovery in a Federal Tort Claims Act case on basis that violation severed bonds of agency); United States v. Casper, 541 F.2d 1275, 1278 (8 Cir. 1976), cert. denied, 430 U.S. 970 (1977) (affirming a finding that violation of the Act does not overcome the presumption of lawful performance of duties by law enforcement officers present); United States v. Wolffs, 594 F.2d 77, 85 (5 Cir. 1979) (holding that a violation would not require the creation of an exclusionary rule for evidence seized in violation of the Act).

46 See, supra, note 27 and accompanying text.

47 William H. Taft IV, Dep’t of Def. Directive 5525.5, DoD Cooperation with Civilian Law Enforcement Officials at 4 ¶ C. (Jan. 15, 1986) (stating applicability to the Navy and Marine Corps “with such exceptions as may be provided by the Secretary of the Navy on a case-by-case basis”); H. Lawrence Garrett III, SecNav Instruction 5820.7B, Cooperation with Civilian Law Enforcement Officials ¶ 9.c. (Navy implementation) (Mar. 28, 1988). See also Donald J. Atwood, Dep’t of Def. Directive 3025.1, Military Support to Civil Authorities ¶¶ B.1., D.4.a., D.4.j. (Jan. 15, 1993) [hereinafter DoDD 3025.1]; William J. Perry, Dep’t of

48 Title 10 U.S.C. § 375 (1998) prohibits direct participation by any member of the armed forces (including the Navy and Marine Corps) in any search, seizure, arrest, or other similar activity; however, unlike the Act, there is no criminal penalty for violating Section 375. Implementing regulation, a DoD directive, prohibits interdiction of vehicles, vessels, or aircraft, apprehension, stop and frisk searches, and surveillance of individuals by military personnel. The Directive also prohibits military personnel from serving as undercover agents, informants, investigators, or interrogators. William H. Taft IV, Dep't of Def. Directive 5525.5, DoD Cooperation with Civilian Law Enforcement Officials encl. 4 ¶ A.3. (Jan. 15, 1986). Section 375, however, only prohibits such activity unless it is otherwise authorized by law, and 10 U.S.C. § 378 (1998) establishes that sections 371-377 (Supp. 1999) do not limit executive authority to act; therefore, those sections do not prohibit any activity that was permissible before their enactment. Since the Navy and Marine Corps were not prohibited from search, seizure, and arrest activity before the enactment, they are not prohibited after. See Rice, supra note 31 at 127 for a full discussion of the application of this exception.


51 See COMMANDER AND THE LAW at 315.

52 One scholar posits that Reserve Officers Training Corps (“ROTC”) cadets are not a part of the Army or Air Force, but United States Military Academy (“West Point”) and United States Air Force Academy (“AFA”) cadets are. Furman at 99. Army and Air Force ROTC cadets called to active duty for summer tours or cruises, advance camp, or field training should be considered a part of the Army or the Air Force.

53 William H. Taft IV, Dep't of Def. Directive 5525.5, DoD Cooperation with Civilian Law Enforcement Officials encl. 4 ¶ B. (Jan. 15, 1986). Active duty members are not acting in a private capacity if they are “induced, required or ordered” by a military official or under the “direction or control” of DoD authorities. COMMANDER AND THE LAW at 315; Taft encl. 4 ¶ B.4. (Jan. 15, 1986). See also OpJAGAF 1976/21, Off-Duty Employment (Mar. 11, 1976) (permitting off-duty employment of Air Force personnel as security guards or auxiliary policemen).


56 Id. at 892 (quoting United States v. Red Feather, 392 F. Supp. 916, 921 (D.S.D. 1975)).

57 Id. (quoting United States v. Jaramillo, 380 F. Supp. 1375, 1379 (D. Neb. 1974), appeal dismissed 510 F.2d 808 (8 Cir. 1975)).

See, infra, notes 135–145 and accompanying text for a discussion of these sections.

Yunis, 681 F. Supp at 894 (citing S. REP. No. 58, 97th Cong., 1st Sess. 148 (1981)).

Yunis, 681 F. Supp at 894.

Implementing regulation describes this “location” authority as “communicating information concerning the relative position of civilian law-enforcement officials and other air and sea traffic.” William H. Taft IV, Dep’t of Def. Directive 5525.5, DoD Cooperation with Civilian Law Enforcement Officials encl. 4 ¶ A.6.b.(4)(a) (Jan. 15, 1986).

Yunis, 681 F. Supp at 894.

Yunis, 681 F. Supp at 894.

Yunis, 681 F. Supp at 895.

Yunis, 681 F. Supp at 895.

Yunis, 681 F. Supp at 895.

Yunis, 681 F. Supp at 895.

Yunis, 681 F. Supp at 895.

Yunis, 681 F. Supp. at 895.

Yunis, 681 F. Supp. at 895.

Yunis, 681 F. Supp. at 895.

Yunis, 681 F. Supp. at 895.

Yunis, 681 F. Supp. at 895.

Yunis, 681 F. Supp. at 895.

See, supra, note 57 and accompanying text.

Yunis, 681 F. Supp. at 895.

See id.

See id.

See id.

See id.

See id.

See, supra, note 79 and accompanying text.

102 Donosa, supra, note 40 at 876.


96 As discussed above, Jaramillo, Red Feather, and McArthur do substantially overlap. McArthur, in particular, refers to both Red Feather and Jaramillo, and considers the overlapping facts and tests of law. United States v. McArthur, 419 F. Supp. 186, 193 (D.N.D. 1975), aff’d sub nom. United States v. Casper, 541 F.2d 1275 (8 Cir. 1976), cert. denied, 430 U.S. 970 (1977). Further, Red Feather refers to and considers Jaramillo. United States v. Red Feather, 392 F. Supp. 916, 921 (D.S.D. 1975). For convenience of reference, the Three Tests, and their subsequent evolved forms, have been associated with the cases in which they were first discussed. To be strictly accurate, more than one of the three cases may support each of the Three Tests.

97 A compulsive action relating to FCC regulations could occur if a military member exceeded actual authority while protecting telephone communications.

98 For example, such an order could be given by a military member to a civilian in a mistaken belief that compliance was required by law or regulation.

99 This paragraph employs the ordinary definitions of “command” and “control,” not the military definitions, where “command” and “control” have special meanings related to troop responsiveness to superior authority, and a particularly special meaning when used conjunctively.

100 For an extended discussion of this concept, see, infra, notes 104–106 and accompanying text.


102 On rare occasion, for example, during the commission of a crime on a federal military reservation by a civilian suspect, military police forces may apprehend suspects on military installations and detain them using citizens’ arrest authority in the appropriate jurisdiction until local law enforcement arrives to arrest those suspects and transport them in custody to law enforcement holding facilities. See, e.g., Eggleston v. Dep’t of Revenue, 895 P.2d 1169, 1170 (Colo. Ct. App. 1995) (“[T]he Act does not prohibit military personnel from acting upon criminal violations committed by civilians on military bases. . . . Specifically, when the actions of military personnel are based on probable cause, the officers are authorized by statute to arrest and detain civilians for on-base violations of state law. . . .”); Richard A. Coleman, Air Force Instruction 31-201, Security Police Standards and Procedures ¶ 7.1.2. (May 1, 1997). In addition to citizens’ arrest authority, a local commander has authority to detain persons not subject to military law until civil authorities can respond. E.g., Donald J. Atwood, Dep’t of Def. Directive 5200.8, Security of DoD Installations and Resources ¶ C.2.d. (Apr. 25, 1991). See also OpJAGAF 1976/72, Posse Comitatus (Oct. 5, 1976) (justifying
some military personnel law enforcement actions relating to on-base violations under the military purpose exception, discussed below in the Military Purpose Exception section in this Part I).

103 See, e.g., William H. Taft IV, Dep’t of Def. Directive 5525.5, DoD Cooperation with Civilian Law Enforcement Officials encl. 4 ¶¶ A.4.b.(1), A.6. (Jan. 15, 1986) (limiting assistance to situations where use of non-DoD personnel would be “unfeasible or impractical from a cost or time perspective”). See also id. ¶ C.2.b. (requiring unavailability of civilian assets and temporary duration of assistance).


105 See, infra, notes 135–146 and accompanying text.


108 See, AFI 36-2501, supra, note 41 at ch. 4.

109 Walden, 490 F.2d at 375.

110 Laird v. Tatum, 408 U.S. 1, 15-16 (1972).

111 Walden, 490 F.2d at 375-76.

112 id.

113 “The Instruction expresses a policy that is for the benefit of the people as a whole, but not one that may be characterized as expressly designed to protect the personal rights of defendants.” Id. at 377 (commenting upon the Instruction applying the Act’s prohibition to Navy and Marine Corps personnel).


116 id.


119 See generally Siemer & Effron, supra, note 23; Donesa, supra, note 40.

120 Compare Restatement (2d) of Foreign Relations Law of the United States § 38 (1965) (stating no extraterritorial effect unless “clearly indicated by the statute”) with Restatement (3d) of the Foreign Relations Law of the United States § 403 com. a (1986) (stating no exercise of jurisdiction “where application of the statute would be unreasonable”) and id. com. f. (stating no extraterritorial application of criminal law unless “express statement or clear implication”) and id. com. g (“interpreting United States law to avoid unreasonable- ness or conflict” with international law).

See id. at 99.

171 F.2d 921, 936 (1 Cir. 1948), cert. denied, 336 U.S. 918 (1949).


See id. at 6. See generally id. at 18-45.


See id. at 6. See generally id. at 18-45.


See generally id. at 18-45.

Siemer & Effron at 54. No case law directly addresses this point, but the authors conclude on the basis of legislative history and principles of statutory construction that the Act is not required to apply extraterritorially. The authors qualify their conclusion with the phrase “[u]nder present circumstances . . . in which no federal civilian agency has a major role in the enforcement of domestic laws overseas . . . .” Id. The increased role of the FBI in the enforcement of domestic law overseas and particularly its increased role in counterterrorism and infrastructure protection may alter the foundation upon which the authors’ conclusion stands. Id. See also Donesa at 882.

Id.


Civilians may be subject to the Code. See Manual for Courts-Martial IV-41 ¶ 28c(1) (1995) [hereinafter MCM] (subjecting civilians to trial by court martial or military commission for aiding the enemy as defined in 10 U.S.C. § 904).

See the section on Civilian Witnesses in Military Investigations in Part III, below.

MCM at II-63-II-67 (R.C.M. 703) (describing production of witnesses and evidence in military jurisdiction criminal cases).


Id. § 372.

Regulation forbids “elaborate” or “large scale” training. William H. Taft IV, Dep’t of Def. Directive 5525.5, DoD Cooperation with Civilian Law Enforcement Officials encl. 4 ¶ A.4.a. (Jan. 15, 1986). However, nothing in the controlling statute forbids large scale training. As a practical matter, the scope of training is a matter of policy, though implementing regulations would need to be changed before large-scale training of civilians by military members would be permissible.


Id.

A joint determination by the Secretary of Defense and the Attorney General is required to invoke this “emergency” clause. Id. See also William H. Taft IV, Dep’t of Def. Directive 5525.5, DoD Cooperation with Civilian Law Enforcement Officials encl. 4 ¶ A.6.b.(4)(b)2 (Jan. 15, 1986).

See, supra, text accompanying note 68.


See, supra, note 48. The chain of logic that results in this outcome is complicated and may not withstand scrutiny under a traditional statutory construction analysis, where a court could consider the express language of the specific prohibition as evidence of congressional intent to affect the Navy and where that court could give relatively lesser weight to a “boilerplate” blanket non-preemption provision that appeared to conflict with the primary intent of the statute. For a detailed discussion setting out the chain of logic to establish this counterintuitive, but possibly valid, outcome see generally Rice, supra, note 31.

See Red Feather discussion notes 59–69 and accompanying text.


Imminently serious conditions resulting from any civil emergency or attack may require immediate action by military commanders, or by responsible officials of other DOD Agencies, to save lives, prevent human suffering, or mitigate great property damage. When such conditions exist and time does not permit prior approval from higher headquarters, local military commanders and responsible officials of other DOD compo-
ments are authorized by this Directive, subject to any supplemental direction that may be provided by their DOD Component, to take necessary action to respond to requests of civil authorities. All such necessary action is referred to in the Directive as Immediate Response.

Donald J. Atwood, Dep't of Def. Directive 3025.1, Military Support to Civil Authorities ¶ D.5.a. (Jan. 15, 1993) (internal quotation marks omitted). See generally John P. White, Dep't of Def. Directive 3025.15, Military Assistance to Civil Authorities (Feb. 18, 1997) (addressing domestic support operations, civil disturbance operations, key asset protection operations, disaster relief operations, operations involving acts or threats of terrorism, and support to civilian law-enforcement agencies); John A. Wickham, Army Regulation 500-51, Emergency Employment of Army and Other Resources: Support to Civilian Law Enforcement (July 1, 1983) (Army implementation); H. Lawrence Garrett III, SecNav Instruction 5820.7B, Cooperation with Civilian Law Enforcement Officials (Mar. 28, 1988) (Navy implementation); Buster C. Glosson, Air Force Instruction 10-801, Assistance to Civilian Law Enforcement Agencies (Apr. 15, 1994) (Air Force Implementation).

156U.S. Const. art. II, § 3.
157See In re Neagle, 135 U.S. 1, 65 (1890); O'Shaughnessy, supra, note 26 at 713.
158See Furman at 92, 97 (commenting that the Act may be unconstitutional as applied to the President, because it conflicts with the inherent Executive authority, but binding as to lesser executive officials, including United States Marshals).
159Acting under the direction of the governor under Title 32 United States Code, and not federalized by declaration of the President under Title 10 United States Code.
161See Rice, supra, note 31 at 109 (discussing the “military purpose doctrine”).
162See Meeks, supra, note 26 at 125.
163Id.
164Id.
165Id.
166Furman, supra, note 26 at 128.
167Meeks at 124–25.
168See id. See also, OpJAGAF 1994/92, OSI (Dec. 30, 1994).
169PDD 63, supra, note 2 at 5.
170Generally speaking, such authority may not be delegated to civilian authorities. See, e.g., Richard A. Coleman, Air Force Instruction 31-201, Security Police Standards and Procedures ¶ 10.2.2. (May 1, 1997). Arguably, the President possesses even broader powers, permitting him to employ federal troops to preserve federal functions and protect federal property, not just military functions and military property. See In re Debs, 158 U.S. 564, 582 (1895) (“[T]he entire strength of the nation may be used to enforce in any part of the land...
the full and free exercise of all national powers and the security of all rights entrusted by the Constitution to its care.). See also William H. Taft IV, Dep’t of Def. Directive 5525.5, DoD Cooperation with Civilian Law Enforcement Officials encl. 4 ¶ A.2.c.(2) (Jan. 15, 1986). Military troops are permitted to provide security for military personnel and assets. For example, Army troops were employed in 1992 after Hurricane Andrew to direct traffic on military supply routes and provide security to food warehouses established by Army Materiel Command. Winthrop, supra, note 154 at 13 n.117.

171While Congress intended to keep military force out of civilian government there is no indication that it meant to affect the Army’s internal administration of the performance of its proper function.” Letter from Mary C. Lawton, Deputy Assistant Att’y Gen., Office of Legal Couns., Dep’t of Just., to Deanne C. Siemer, Gen. Couns., Dep’t of Def. (Mar. 24, 1978) (quoted in Siemer and Effron, supra, note 23 at 14 n.47) (internal quotation marks omitted) (discussing investigation and prosecution of frauds perpetrated by civilians who had entered into contracts with military departments).


175JV 2010 at 3 (discussing the present and future role of the military services). See also, THE WHITE HOUSE, A NATIONAL SECURITY STRATEGY FOR A NEW CENTURY 2-3 (1998) (describing the essential and intrinsic national security goal to protect the safety of citizens, the security of America’s borders, and America’s critical infrastructures)

176Sparseness of case law on this precise point precludes an analysis of precedent; however, a common standard of scrutiny for government action taken by administrative officials is the “arbitrary and capricious test,” also referred to as the “abuse of discretion test” or the “rational basis test.” See 5 U.S.C. § 706(2)(A) (1996) (setting out the test). See also Motor Vehicle Mfrs. Ass’n v. State Farm Mutual Auto. Ins. Co., 463 U.S. 29, 43 (1983) (holding an agency rule is arbitrary and capricious if the agency action relied on factors Congress did not intend, failed to consider an important aspect of the problem, contravenes the evidence, or is so implausible it cannot result from differing views or expertise). Further, DoD policy governing the military-civilian interface in a law enforcement context requires that “[A]uthority must not be exercised in an arbitrary, capricious, or discriminatory manner. . . . [A]ctions must be based on reasonable grounds and be judiciously applied.” Donald J. Atwood, Dep’t of Def. Directive 5200.8, Security of DoD Installations and Resources ¶ C.2.c. (Apr. 25, 1991).

177JOINT CHIEFS OF STAFF, CONCEPT FOR FUTURE JOINT OPERATIONS: EXPANDING JOINT VISION 2010 83 (1997) [hereinafter EJV 2010].

178Id. at 65.

179Id. at 66.

180JV 2010, supra, note 174 at 19-27. “Dominant maneuver will allow our forces to gain a decisive advantage. . . .” Id. at 20. “Precision engagement will allow us to shape the
battlespace, enhancing protection of our forces.” Id. at 21. “Full-dimensional protection will enable the effective employment of our forces while degrading opportunities for the enemy.” Id. at 22. “Focused logistics will enable joint forces . . . to be more mobile, versatile, and projectable from anywhere in the world.” Id. at 23. “[T]hese four new concepts will enable us to dominate the full range of military operations. . . .” Id. at 25.

181Id. at 13 (“Improvements in information and systems integration technologies will also significantly impact future military operations. . . .”). See also EJV 2010 at 9 (“Information technology will be vital to military operations. . . .”).

182See EJV 2010 at 50, 52, 53, 54 (1997). “Information superiority is what makes dominant maneuver a new concept. . . .” Id. at 50. “Information superiority will allow information-based control to displace physical control of [military] forces. . . .” Id. “Likewise, information superiority enables precision engagement. . . .” Id. at 52. “Like the other new concepts, full-dimensional protection requires information superiority. . . .” Id. at 53. “Information Age technologies—particularly information specific technologies that provide information superiority—will enable the new concept of focused logistics.” Id. at 53.

183Id. at 24.

184Id. at 39.

185See JV 2010 at 24 (“Defense agencies will work jointly and integrate with the civilian sector, where required, to take advantage of advanced business practices, commercial economies, and global networks.”); EJV 2010 at 55 (“Service and defense agencies will work with the civilian sector to take advantage of advanced business practices, distribution processes, materiel management programs, and global networks.”). See also, e.g., id. at 56 (“[F]ocused logistics is characterized by . . . [v]isibility of commercial, multinational, [nongovernmental organization], and [private volunteer organization] capabilities and sources of supplies and services.”).


187Michael Vickers, Director of Strategic Studies, Center for Strategic and Budgetary Assessment, Wash. D.C., Remarks at the Center for International Security and Cooperation, Stanford University, on New Challenges to U.S. Security (May 25, 1999).

188EJV 2010 at 36, 84.

189EJV 2010 at 85. “[I]nformation infrastructure] includes three categories: global information infrastructure (GII), national information infrastructure (NII), and defense information infrastructure (DII).” Id.

190In PDD 63, the President orders government agencies to ensure that interruptions or manipulations of critical functions be brief, infrequent, manageable, geographically isolated, and minimally detrimental. Critical functions include essential national security missions, general public health and safety, minimum essential state and local public services, orderly functioning of the economy, and delivery of essential telecommunications, energy, financial, and transportation services by the private sector. PDD 63, supra, note 2 at 2.

191Id. at 9.

192Id. at 10.


See Annapolis Speech, supra, note 6.

PDD 63 designates lead agencies for the special purposes of national defense (DoD), foreign affairs (Department of State), intelligence (Central Intelligence Agency), and law enforcement (Department of Justice and FBI). Id. at 4, 8. Efforts of those lead agencies along with those of other agencies and other organizations coordinate to implement PDD 63 under the auspices of the Critical Infrastructure Coordination Group (“CICG”), chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. Id. at 4–5. The wide net of oversight cast by the CICG and National Coordinator are indicative of the extensive level of interagency cooperation that will be required to establish and maintain infrastructure security.

PDD 63 at 10.


Id. at 482 (internal quotation marks omitted).


Id.

See id. at 113 (finding that the flight was scheduled for the purpose of training the military crew and maintaining the skills of the crew).

See id. at 115 (noting that the military pilot diverted from the planned course only when diversion did not interfere with the training mission, but refused to divert when diversion would interfere with the mission’s objectives).
At the express direction of Congress, the military services are authorized to enforce against military members, but generally not civilians, criminal laws contained in the Uniform Code of Military Justice. See 10 U.S.C. § 802(a). But see, supra, note 132 (noting that civilians may be subject to the Code).


A military purpose attack could appear even more “civilian-targeted” if the source attacks a commercial-off-the-shelf government contractor doing business with the military under Federal Acquisition Regulation part 15. See, infra, note 248 and accompanying text (discussing FAR 15). One hypothetical but plausible scenario would be an attempted compromise of internal communications at, for example, Cisco Systems, a prominent network hardware manufacturer, in an attempt to sniff out possible vulnerabilities in Cisco routers, hubs, and switches, the vulnerabilities of which an attacker could exploit against military communications networks employing such products.

Network audit logs and telecommunications modem pool logs helped America Online and law enforcement officials track down the man who released the Melissa macrovirus in March 1999. The ability to identify the computer from which the virus originated using Microsoft’s Global Unique Identifier, enabled by some Microsoft Word implementations, also assisted in an expedient and successful investigation. Joel Deane, Melissa Manhunt Creates Precedent, ZDNN TECH NEWS NOW (Apr. 6, 1999) available at <http://www.zdnet.com/zdnn/stories/news/0,4586,2237838,00.html>.


Solar Sunrise involved unauthorized access to DoD computer systems. Melissa involved unauthorized commandeering of email accounts to resend a virus. Solar Sunrise was a real-time attack. Melissa was predominantly a propagating attack, time-delayed by the store-and-forward nature of email. While switching equipment designed to enable real-time tracking would have assisted in the Melissa investigation, the ability to trace unauthorized access in real time would have been more directly applicable to Solar Sunrise.


See, supra, note 212.

Denning describes sniffers as “programs that, installed on network nodes, intercept packets traversing the network and ferret out login IDs and passwords, credit card numbers, or
messages containing certain keywords.” Supra, Protection and Defense, note 212 at text accompanying n.6.

An attacker with high-level insider access (“root” or “superuser” access) can easily destroy or modify files. Attacks using high-level access to computers containing routing tables and other network controls may disrupt operations on an entire network. In contrast, an outsider is generally limited to using the speed and connectivity of the network against the target, assailing the target using the target’s ports to the network, or launching denial of service attacks. Even low-level insider access can be of assistance to such “outsider” attacks by occupying system resources, diverting system administrator attention, and opening ports to the outside.


See, supra, note 169 and accompanying text.

See, supra, note 220 and accompanying text.


O’Callahan has been overruled as described above in note 224. The fact that the rule in O’Callahan is no longer binding is irrelevant to the analogy drawn in this section. When the rule in O’Callahan was binding, it created a dilemma for the commander. The fact that modern commanders do not face O’Callahan dilemmas does not preclude comparison of the modern commander’s infrastructure protection dilemma to a predecessor’s O’Callahan dilemma. The reasoning that permitted the predecessor to resolve the O’Callahan dilemma also permits the modern commander to resolve the infrastructure protection dilemma. The Gosa decision, described below in note 232 and the accompanying text, is much more important to the continued vitality of the analogy. Gosa’s holding relating to the lack of a definitive jurisdictional boundary permits a commander to resolve uncertainty by actively investigating until a more definitive decision can be made regarding the proper forum.

Defined, supra, text accompanying note 131. The UCMJ is a statutory exception to the prohibitions of the Act, permitting military personnel to enforce the laws required to maintain good order and discipline. See Furman, supra, note 26 at 104.

395 U.S. at 274.

See, supra, note 26 at 105.

See, e.g., supra, note 166 and accompanying text.

See, supra, notes 59–69 and accompanying text.

Meeks at 105.


Meeks at 105 (citing Munnecke, O’Callahan Revisited and Buttoned Up, 46 Judge Advocate’s J. 11 (1974)).

Id.

Under PDD 63, coordination with the FBI regarding infrastructure attacks is required. While timing is not specified in President Clinton’s directive, such coordination should begin as soon as practicable, and in any event within a reasonable time, even if the military pur-
pose remains primary. See, supra, note 198 and accompanying text. See also W. Graham Clayton, Dep't of Def. Directive 5200.27, Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense ¶ F.1. (Jan. 7, 1980) (“Nothing in this Directive shall be construed to prohibit the prompt reporting to law enforcement agencies of any information indicating the existence of a threat to life or property, or the violation of law, nor to prohibit keeping a record of such a report.”).

236 Regulatory limitations . . . do not preclude [military members] from conducting preliminary inquiries or investigations to determine whether fraud or other suspected criminal conduct falls under the Air Force or the FBI investigative and prosecutive jurisdiction.” OpJAGAF 1977/27, Posse Comitatus ¶ C. (Apr. 8, 1977). See also United States v. Griley, 814 F.2d 967, 976 (4 Cir. 1987) (“Because it was not known whether the thieves were military personnel or civilians, the Army’s CID worked with the FBI in investigating the thefts.”)

237 See OpJAGAF 1977/27, Posse Comitatus ¶¶ B., C. (Apr. 8, 1977) (permitting collateral investigations by military personnel of contractor fraud to protect federal property or functions while civilian criminal investigations are under way).

238 Furman, supra, note 26 at 113.

239 Id.

240 If the subject of the warrant or subpoena is the property or person of a military member, and the military purpose of the investigation is primary, issue of military search authorizations by a military magistrate and execution by military personnel is proper in accordance with regulatory guidance. See, e.g., William K. At Lee Jr., Air Force Instruction 51-201, Administration of Military Justice ¶ 3.1.4. (Oct. 3, 1997). However, use of the UCMJ subpoena power of military trial counsel to command production of documents held by civilians or command civilian presence at trial may be appropriate and proper, if applicable. See, supra, note 134 and accompanying text.

241 Furman at 105.

242 Furman at 105–06.

243 See, supra, notes 153–154 and accompanying text.

244 W. Graham Clayton, Dep’t of Def. Directive 5200.27, Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense ¶¶ D.1.c., D.1.f. (Jan. 7, 1980).


246 See, id. at 503, 505, 506.

247 Id. at 511.


250 Listservers are threaded electronic discussion forums. A threaded discussion is one where a participant can filter out unrelated discussions posted to the same forum by following an electronic “thread” between related messages.

Poulsen’s case appeared to be primarily a law enforcement case, and incidentally a national security concern, but, under the analysis set out in this article, military involvement—focused on the compromise of classified military information and preventing similar future compromises—would have been permissible, so long as law enforcement personnel had control over the portions of the investigation related to the gathering of evidence necessary for Poulsen’s prosecution.

See, supra, note 176 (discussing application of rational basis test).

See, supra, note 17 and accompanying text.


See, supra, text accompanying note 99.

See, supra, notes 54–58 and accompanying text.

But see, supra, note 96 and accompanying text regarding possible violations through the exercise of regulatory, compulsory, or proscriptive power or the active direct enforcement of non-criminal law when no crime has been committed.

WHITE HOUSE, DEFENDING AMERICA’S CYBERSPACE: NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION (VERSION 1.0) 25–29 (May, 1999) [hereinafter NATIONAL PLAN].


Implementing these concepts in computer security should not be restricted to the traditional “unclassified,” “secret,” and “top secret” system in current use. Separating and “classifying” system-control related programs and data that an ordinary user would have no need to see or use is one such extension of the classification and compartmentalization concept.

In peacetime, responsibility for protecting non-DoD Critical Assets and designing their security rests primarily with the civil sector owners and with local, State, and Federal law enforcement authorities. However, the Department of Defense must participate with the civil sector, emergency preparedness and law enforcement authorities in planning for Critical Asset assurance during an emergency, and must be prepared, in concert with the appropriate authorities and within defense priorities, to assist in their protection during physical or technological attack, and technical or other emergency that seriously degrades or threatens DoD operations.

See, supra, note 96 and accompanying text.

NATIONAL PLAN at 46. The First and Second Detail ERTs contained one DoD security expert each. Id. at 49.

See NATIONAL PLAN at 46, 67.


The National Plan proposes that FIDNET be built using netted adaptive intrusion detection technology. See NATIONAL PLAN at 15, 67-70.

It is possible that, for caseload or other reasons, the FBI or another law enforcement agency may delay in adopting and actively pursuing an investigation handed off from a military service. Therefore, the point where it reasonably appears that the civilian forum is proper may be significantly earlier than the point where civilians begin to investigate. Nevertheless, when the civilian forum is proper, military personnel may not actively investigate except for a military purpose, such as determining method of attack to protect military interest systems against future attack. Military members cannot become principal investigators of civilian criminal activity for the purpose of preparing a criminal case against perpetrators. To do so would violate the Act’s prohibitions, even if civilian criminal investigators are not vigorously pursuing the case. Encouraging civilian investigators to work on a case would not, however, be a violation of the Act.

For example, one Air Force Legal Information Services logon greets telnet visitors:

This is a Department of Defense computer system for authorized use only. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate against unauthorized access, and to verify security procedures, survivability, and operational security. Using this system constitutes consent to monitoring. All information, including personal information, placed on or sent over this system may be obtained during monitoring. Unauthorized use could result in criminal prosecution.

Notice of security regulations may be required by statute and DoD regulation. See 50 U.S.C. § 797(b) (1991); Donald J. Atwood, Dep’t of Def. Directive 5200.8, Security of DoD Installations and Resources ¶ E.2. (Apr. 25, 1991) (“[M]ilitary commanders shall . . . conspicuously post . . . security orders and regulations issued . . . to ensure proper safeguarding of personnel, facilities, and property from loss, destruction, espionage, terrorism or sabotage.”)

Industry information sharing and assessment centers (“ISACs”) are described in the PCCIP Report, PDD 63 and the National Plan. See, PCCIP REPORT, supra, note 1 at 57–58; PDD 63, supra, note 2 at 10–11, NATIONAL PLAN at 91. See also NATIONAL PLAN at 44 (describing DoD interface with ISACs).


486 F. Supp. 1348 (M.D.Fla. 1980), aff’d, 679 F.2d 961 (11 Cir. 1982).
274] Id. at 1351.
275] Id. at 1357 n.14.
276] See Meeks at 113.
278] See id.
280] See also, supra, note 236.
282] See 10 U.S.C. § 372 (1998). This section deals with assistance in the context of drug, immigration and customs law enforcement. For a discussion regarding the applicability of this section outside those contexts, see, supra, note 146 and accompanying text. See also, United States v. A. Hartley, 796 F.2d 112, 115 (5 Cir. 1986) (finding that military members “provided only information regarding the movement of an unidentified aircraft entering the United States”).
284] See, supra, note 198 and accompanying text (discussing President Clinton’s PDD 63 mandate to cooperate).
286] Such USENET groups are threaded listserv discussions available to the public using “newsreader” software.
288] Id. at 377.
289] Laird v. Tatum, 408 U.S. 1, 15–16 (1972). In Laird, where the Supreme Court spoke to surveillance of war protestors by U.S. Army Intelligence operatives in preparation to quell a potential civil disorder, the Court rejected the lower court’s “broad sweep[ing]” holding. The lower court had held judicial review of such surveillance proper. The Laird Court stated that such monitoring of the wisdom and soundness of Executive policy decisions is charged to Congress, not the judiciary. The Court disposed of the case by holding that the protesters had not suffered a cognizable injury, but noted “a traditional and strong resistance of Americans to any military intrusion into civilian affairs” and warned that “there is nothing . . . in our holding today that . . . give[s] any indication that actual or threatened injury by reason of unlawful activities of the military would go unnoticed or unremedied.” Id.
291] See, supra, note 270 and accompanying text.
See, supra, note 289 and accompanying text. See also Ex parte Milligan, 71 U.S. (4 Wall.) 2, 124 (1866). Under Laird, surveillance of civilians by military members does not give rise to a cognizable injury, so long as the activity of military members is lawful; nevertheless, DoD policy disfavors surveillance of civilians even if lawful. See Laird, 408 U.S. at 15–16; William H. Taft IV, Dep't of Def. Directive 5525.5 DoD Cooperation with Civilian Law Enforcement Officials, encl. 4 ¶ A.3.d. (Jan. 15, 1986) (prohibiting use of military personnel for surveillance of individuals to assist civilian law-enforcement personnel).

Such protection includes combating theft, destruction, or sabotage of DoD facilities, equipment, or records; investigating direct threats to DoD personnel; protecting key defense facilities, classified defense information, or facilities executing classified defense contracts; countering unauthorized demonstrations on DoD installations; and averting subversion of loyalty, discipline, or morale of DoD personnel. W. Graham Clayton, Dep't of Def. Directive 5200.27, Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense ¶ D.1. (Jan. 7, 1980).

¶ D.2. (requiring such personnel to be employees of DoD or to require access to sensitive information).

¶ D.3. (requiring authorization from the Secretary of Defense).


Id. (internal quotation marks omitted).

See, supra, note 146 and accompanying text.

National Plan, supra, note 258 at 53–54.


National Plan at 61, 63.

Cf. OpJAGAF 1984/17, Posse Comitatus (Mar. 13, 1984) (permitting passive advisory assistance to National Narcotics Border Interdiction System centers, but forbidding active participation as “case agents,” presumably because there is no military purpose).

McArthur at 195.

Legitimate use of military force to suppress insurrection would have required an order of the President under 10 U.S.C. 331–334 (1998).

McArthur at 195.

See, supra, note 154.
NATIONAL PLAN, supra, note 258 at 43. Topics include infowar basics, infosec awareness, an overview of information technology infrastructures, information assurance for auditors and evaluators, and hacker intrusion methods. Id.

See William H. Taft IV, Dep't of Def. Directive 5525.5, DoD Cooperation with Civilian Law Enforcement Officials encl. 4 ¶ A.2.a.(3) (Jan. 15, 1986)


The military purpose exception was known at the time, but the court did not address such a good order and discipline argument. Such an argument may not have been made or considered substantial enough to mention in the opinion. There was no discussion by the court about actual military purchases in violation of law or a problem with illegally purchased guns on base.


DENNING, supra, note 251 at 392–93.

If the military objective is simply to expel intruders and repel an attack, care should be taken pursuant to the Law of Armed Conflict principles of necessity and proportionality to use no more force than reasonably necessary and to avoid disproportionate collateral damage. See OFFICE OF THE JUDGE ADVOCATE GENERAL, DEPARTMENT OF THE AIR FORCE, LAW OF ARMED CONFLICT TRAINING GUIDE 33–35, 49 ¶ 3–8 (1993).


But see id.

But see, supra, note 102 (regarding permissible temporary apprehension and detention of civilians pending delivery to civilian law-enforcement officials).

But see, supra, note 134 regarding military trial counsel subpoena power and military magistrate search authorizations.

But see, supra, note 132 regarding applicability of the Code and jurisdiction of the military over civilians.

See, supra, notes 131–134 and accompanying text.

Wrynn v. United States, 200 F. Supp. 457, 459 n.1 (E.D.N.Y. 1961). The commander told his troops that they could voluntarily return to assist the posse as citizens in their personal private capacities, but refused to command them as military members to search for the prisoner. Id.

Id. at 465. The result differs if the criminals at large are military members or if fleeing felons are actually on a military reservation and pose a threat to the military community. See,
e.g., Harker v. State, 663 P.2d 932, 932, 937 (Alaska 1983) (“[T]he military has a legitimate independent interest in protecting persons on base from fleeing armed felons. . . .”).

Subject, of course, to classification or other dissemination restrictions.

DoD policy requires consideration of potential for use of lethal force by or against DoD forces, safety of DoD forces, cost, the interest of DoD, and the impact of DoD’s ability to perform its primary mission. See John P. White, Dep’t of Def. Directive 3025.15, Military Assistance to Civil Authorities ¶ D.2. (Feb. 18, 1997).


Supra, note 35.

See, supra, note 289 and accompanying text.


For example, “air superiority” in “airspace” permits more effective application of sea and ground forces. Likewise, “information superiority” in the “information battlespace” permits more effective application of air, sea, and ground forces. See, J V 2010, supra, note 174 at 17.

United States v. M cArthur, 419 F. Supp. 186, 193–94 (D.N.D. 1975), aff’d sub nom. United States v. Casper, 541 F.2d 1275 (8 Cir. 1976), cert. denied, 430 U.S. 970 (1977) (“It is the nature of their primary mission that military personnel must be trained to operate under circumstances where the protection of constitutional freedoms cannot receive the consideration needed in order to assure their preservation.”).

Notable exceptions are military police and investigative forces (e.g., Air Force Security Forces, Army Military Police, Navy Shore Police, Air Force Office of Special Investigations, Army Criminal Investigation Division, and Naval Investigative Service), which are trained to accomplish law enforcement missions and police Special Weapons and Tactics (“SWAT”) teams, which are trained to handle high-firepower confrontations that more frequently involve application of lethal force. Military police are well versed in the protection of individual liberties and Constitutional rights. In fact, military members are arguably entitled to more expansive rights against self-incrimination under Article 31, Uniform Code of Military Justice, than the Miranda decision provides civilians. See 10 U.S.C. § 831 (1998).

E.g., Jesse Katz, A Good Shepherd’s Death, L.A. T im es, June 21, 1997, at A1 (describing a fatal mistake made while troops were employed for border patrol); See also, e.g., Border Killing Brings Criticism of Military Role, C hic ago T rib., May 23, 1997, at 15.


BLACK’S LA W DICTIONARY at 1599.

O’Shaughnessy, supra, note 26 at 731 n.171.

Fields v. United States, 164 F.2d 97, 100 (D.C. Cir. 1947) (quoting Townsend v. United States, 95 F.2d 352, 358 (D.C. Cir. 1938), cert. denied, 303 U.S. 664 (1938), and American Surety Co. v. Sullivan, 7 F.2d 605, 606 (2 Cir. 1925)) (internal quotation and editing marks omitted), cert. denied, 332 U.S. 851 (1948).


Id. at 818-19.

See id. at 817-18 (stating that “bare allegations of malice” are insufficient to justify the burden of discovery upon a government servant).

See, supra, notes 107-118 and accompanying text.

See id. at 818.


Annapolis Speech, supra, note 6 (addressing cyber terrorism).


Deutch Lecture, supra, note 155 (addressing “catastrophic terrorism”).
To order, call (650) 725-6488 or fax (650) 723-0089. Selected publications and a complete publications list are also available on the Center’s website: www.stanford.edu/group/CISAC/.

Herbert L. Abrams. Can the Nation Afford a Senior Citizen As President? The Age Factor in the 1996 Election and Beyond. 1997.


George Bunn. The Nonproliferation Regime under Siege. 1999.


Amos Kovacs. The Uses and Nonuses of Intelligence. 1996.


Terence Taylor. Escaping the Prison of the Past: Rethinking Arms Control and Non-Proliferation Measures. 1996.


Dean A. Wilkening. The Evolution of Russia's Strategic Nuclear Forces. 1998.


MacArthur Consortium Working Papers in Peace and Cooperation


Daniel T. Froats. The Emergence and Selective Enforcement of International Minority-Rights Protections in Europe after the Cold War. 1996.


Bruce A. Magnusson. Domestic Insecurity in New Democratic Regimes: Sources, Locations, and Institutional Solutions in Benin. 1996.