I. INTRODUCTION

With awareness of the contemporary data insecurity and critical infrastructure vulnerability crises seemingly ever-increasing, there has been a scramble recently to adapt governmental instrumentalities to meet the threats that now unquestionably constitute one of the major defense challenges facing the United States. At times, these efforts at progress have butted up against existing legal frameworks and principles, making the effectuation of changes in policy a more complicated endeavor. As the government seeks to exercise more control over cyberspace, an effort that necessarily impacts substantive rights guarantees and various

* Harvard Law School, J.D. Candidate, 2011.
3 See DEPARTMENT OF DEFENSE, QUADRENNIAL DEFENSE REVIEW REPORT 8 (2010).
6 See Winnefeld & Alexander Hearing, supra note 4, at 12 (testimony of Lt. Gen. Alexander) (“Civil liberties, privacy all come into that equation, ensuring . . . privacy while you try to . . . take care of bad actors [is a] difficult problem.”).
interlocking legal frameworks, this trend is likely to continue.

One aspect of the law potentially implicated by current and future governmental action in the cybersecurity field is the legal and regulatory framework built around the Posse Comitatus Act, a bill originally created during the Reconstruction era, which has served as the positive law-basis for the principle that the American people should not be subjected to the force of the American military in the law enforcement context. The Posse Comitatus Act, coupled with accompanying pieces of legislation and regulation, establishes a set of limits on what the military can and cannot do on American soil. In seeking to increase governmental power in the cybersecurity field, actions have already been taken that may impact well-established Posse Comitatus principles, and the likely future course of governmental action is apt to bring about further conflicts of this sort. Understanding what the Posse Comitatus Act does and does not restrict within this field is thus crucial in the context of developing coherent and legally sound policy responses to the cybersecurity crisis in which the United States now finds itself.

This paper will seek to address the Posse Comitatus Act implications of developments in the federal government’s approach to cybersecurity. It will first set out the basic legislative and

7 Consider, for example, the controversy over the Federal Communications Commission’s recent decision to classify the transmission component of broadband access service as a telecommunication service instead of as an information service. See Hiawatha Bray, FCC reasserts its power to regulate Internet providers, BOSTON GLOBE, May 7, 2010, at 5. See generally JULIUS GENACHOWSKI, CHAIRMAN, FEDERAL COMMUNICATIONS COMMISSION, THE THIRD WAY: A NARROWLY TAILORED BROADBAND FRAMEWORK (May 6, 2010), http://www.broadband.gov/the-third-way-narrowly-tailored-broadband-framework-chairman-julius-genachowski.html.
11 See generally infra Part III.
12 See generally infra Part VI.
regulatory structure that underlies present Posse Comitatus law as it relates to cybersecurity. It will then turn to address the Posse Comitatus Act ramifications of the creation of U.S. Cyber Command, before also treating the question of how related changes in the role of the government in cybersecurity will implicate Posse Comitatus principles—to wit, military protection of private networks, and offensive cyber-operations by the military against targets in the homeland, both of which are endorsed with varying degrees of explicitness in the 2010 Quadrennial Defense Review. Finally, it will analyze the Posse Comitatus implications of the various pieces of cybersecurity legislation now moving through Congress, the Rockefeller Bill in particular. Note that this paper will not address the legality or constitutionality of the various governmental actions under consideration in any comprehensive way—it will deal only with the issue of conflicts with the current Posse Comitatus legal regime.

II. The Posse Comitatus Act

The Posse Comitatus Act draws its name from a common law power of state agents to call forth the posse—or power—of their comitatus—a medieval term meaning both an armed retinue and an administrative unit of government. At the common law, a local sheriff had the right to summon every able-bodied commoner residing in his jurisdiction to help enforce the law. This “posse” included military personnel—in fact, Blackstone defined the sheriff’s power to pursue criminals with the posse comitatus as co-extensive in scope with his power to repel attacks “of the king’s enemies.”

---

14 See DEPARTMENT OF DEFENSE, QUADRENNIAL DEFENSE REVIEW REPORT (2010).
16 See 1 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 331–32.
17 Id. at 332.
Contrarily, federal law in the early days of the Republic embraced the basic principle that standing armies raised by Congress should not operate against Americans in the law enforcement context. Over time, though, there was significant erosion of this principle, and by the mid-19th century military personnel in their personal capacity and, more significantly, organized military forces subordinated to civil authority were accepted members or components of the posse. This practice became particularly pronounced after the Civil War, when outright military government of the Southern states was implemented for a time, after which military forces continued to make themselves an intrusive presence in the governing and policing of the regions in which they found themselves stationed. The Posse Comitatus Act of 1878 followed in the wake of the “Corrupt Bargain,” which won Rutherford B. Hayes the White House at the cost of ending Reconstruction. The Act limited the use of the Army “for the purpose of executing the laws” to instances covered by a specific Congressional or Constitutional mandate. Thus, in the absence of positive law to the contrary, the Army was barred from acting in the domestic law enforcement context. Significantly, the Navy was not similarly constrained—the original Posse Comitatus Act was included as a provision in an Army spending authorization, and thus only applied to the Army.

The Posse Comitatus Act has been subject to various amendments and changes over the

---

19 See id; see also S. Rep. No. 31-320, at 1 (1852) (“Because men are soldiers or sailors, they cease not to be citizens; and while acting under the call and direction of the civil authority, they may act with more efficiency, and without objection, in an organized form, under appropriate subordinate command.”).
23 See id.
course of its history, most notably the extension of its ambit to cover the Air Force, but in basic form it retains its 1878 structure and purpose:

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 not more than two years, or both.

Although federal courts long refused to apply the Act to the Title 10 military branches not therein listed, namely the Navy and Marine Corps, Congress has implicitly called for the extension of Posse Comitatus principles to cover the entire Title 10 military. 10 U.S.C. § 375 calls for the Secretary of Defense to issue rules so as to prevent “direct participation by a member of the Army, Navy, Air Force, or Marine Corps in a search, seizure, arrest, or other similar activity unless participation in such activity by such member is otherwise authorized by law.” Although no civil or criminal remedy is provided for a failure on the part of the Secretary to so regulate, potentially raising a question as to § 375’s legal cognizability, Department of Defense Directive 5525.5, entitled “DoD Cooperation with Civilian Law Enforcement,” brings Defense Department policy into line with the requirements of both the

---

26 See, e.g., United States v. Yunis, 924 F.2d 1086, 1093 (D.C. Cir. 1991) (upholding a district court’s refusal to dismiss a criminal action on Posse Comitatus grounds because of support rendered by the Navy to an FBI operation, as “[b]y its terms, [the Posse Comitatus Act] places no restrictions on naval participation in law enforcement operations”).
28 See id.
29 It has been previously argued that the lack of such a remedy in § 375 means that the Secretary of Defense could modify DoDD 5525.5 to exclude the Navy and Marine Corps from its ambit, freeing them to participate in law enforcement unreservedly, without subjecting himself to any possible legal penalty. See Linda J. Demaine & Brian Rosen, Process Dangers of Military Involvement in Civil Law Enforcement: Rectifying the Posse Comitatus Act, 9 N.Y.U. J. LEGIS. & PUB. POL’Y 167, 175–76 (2005).
Posse Comitatus Act and § 375.30

Pursuant to the exception clause of the Act, federal law currently recognizes six general areas in which either the Constitution or statutes supersede Posse Comitatus.31 (1) In cases of civil disturbances, national disasters, or “calamities,” actions taken by military forces in contravention of Posse Comitatus “to prevent loss of life or wanton destruction of property and to restore governmental functioning and public order” are authorized.32 (2) Where local authorities are unable, the use of military forces to protect federal property and federal governmental functions is allowed.33 (3) When a state is unable to control domestic violence and it requests federal assistance to deal with the same, federalized militia and the armed forces can be called into service for that purpose.34 (4) Where a rebellion makes the enforcement of the law impossible, federalized militia and the armed forces can be used to enforce the law and suppress the rebellion.35 (5) Where an insurrection impedes the enforcement of the law in a manner that leads to a rights deprivation for a class of people, and where state authorities are unable to

\[30\] See Dep’t of Def., Directive No. 5525.5, DoD Cooperation with Civilian Law Enforcement Officials 1, § 2.2 (1986) (incorporating Change 1, Dec. 20, 1989) [hereinafter DoDD 5525.5] (defining applicability with regard to the term “Military Service,” therein defined as “the Army, the Navy, the Air Force, and the Marine Corps”).


\[32\] 32 C.F.R. § 215.4(c)(1)(i) (the “emergency authority”).

\[33\] Id. at § 215.4(c)(1)(ii).


protect, or refuse to protect, those rights, federalized militia and the armed forces can be used to suppress the insurrection. Finally, (6) on request of the Secret Service, all government departments and agencies including the service branches are required to assist in the protection of government officials and major political candidates. Furthermore, it is generally accepted that the Posse Comitatus Act does not apply extraterritorially, in part because of the President’s Take Care obligations and the presumption that the military will at times constitute the President’s only instrumentality to enforce the law overseas.

Even beyond these six areas of clear exception, the Posse Comitatus Act only restricts the use of covered personnel from a specific class of activity, namely the “execution of the laws.” Disagreements within the federal judiciary over what constitutes this class of activity have at times been pronounced, but the dominant standard seems to be well-established enough at this point to consider it authoritative, despite it never having reached the Supreme Court.

In the litigation that followed the use of the 82nd Airborne Division to clear armed protesters out of Wounded Knee, South Dakota in 1973, three federal district courts adopted three different standards to define prohibited activity under the Posse Comitatus Act: one based on an active/passive activity distinction, the second on a determination as to the degree to

---

41 It is rather difficult to find objective accounts of Wounded Knee II. The two best sources, each quite biased in favor of one party or the other, appear to be JOSEPH H. TRIMBACH & JOHN M. TRIMBACH, AMERICAN INDIAN MAFIA (2007), and VOICES FROM WOUNDED KNEE, 1973 (1974).
which military action had “pervaded” the law enforcement activities at issue, and the third on the basis of a test as to whether civilians had been subjected to military actions “regulatory, prescriptive or compulsory in nature.” The Office of Legal Counsel regularly cites all three District Court standards together in its opinions.

The language of the third test is borrowed from Supreme Court First Amendment jurisprudence. In Laird v. Tatum, the Supreme Court addressed the issue of whether the mere existence of a government surveillance program could chill speech in such a way so as to give rise to a justiciable controversy. The Court held that, absent actions that were “regulatory, prescriptive, or compulsory” in nature, allegations of a subjective “chill” were not sufficient to support a claim.

This “regulatory, prescriptive, or compulsory” standard was adopted by the Eighth Circuit Court of Appeals in preference to the other two district court rules in Casper, and developed further by the same court in Bissonette. In the latter case, the court held that “military involvement [in law enforcement], even when not expressly authorized by the Constitution or a statute, does not violate the Posse Comitatus Act unless it actually regulates, forbids, or compels some conduct on the part of those claiming relief. A mere threat of some


46 See Bissonette v. Haig, 776 F.2d 1384, 1390 (8th Cir. 1985) (“This formulation [in McArthur] is based on language found in . . . Laird v. Tatum”).

47 Laird v. Tatum, 408 U.S. 1, 11 (1972).

48 United States v. Casper, 541 F.2d 1275 (8th Cir. 1976).

49 Bissonette v. Haig, 776 F.2d 1384 (8th Cir. 1985).
future injury would be insufficient.”

Other courts have treated this framework favorably, including the Fourth, \textsuperscript{51} Fifth, \textsuperscript{52} and Eleventh \textsuperscript{53} Circuit Courts of Appeals, and it forms the core of the Department of Defense’s regulatory regime articulating the Posse Comitatus Act. \textsuperscript{54}

DoDD 5525.5 establishes as Department of Defense policy cooperation with “civilian law enforcement officials to the extent practical [and] consistent with the needs of national security and military preparedness, the historic tradition of limiting direct military involvement in civilian law enforcement activities, and the requirements of applicable law.” Congruent with the requirements of the Posse Comitatus Act, DoDD 5525.5 establishes strict restrictions on the use of Defense Department personnel for civilian law enforcement.

Enclosure 4 enumerates the standards for permissible direct assistance\textsuperscript{56} and for prohibited direct assistance.\textsuperscript{57} Actions taken primarily to further a military or foreign affairs function are permissible, even where they also impact civilian law enforcement in an otherwise proscribed manner.\textsuperscript{58} Relying on this military function distinction, an October 23, 2001 Office of the Legal Counsel (OLC) opinion on the legality of using the military to combat terrorists on American soil concluded that Posse Comitatus would not apply to military personnel so deployed, as “domestic military operations against potential attacks on the United States” are not

\textsuperscript{50} Id. at 1390.

\textsuperscript{51} See United States v. Al-Talib, 55 F.3d 923, 930 (4th Cir. 1995).

\textsuperscript{52} See United States v. Allred, 867 F.2d 856, 870–71 (5th Cir. 1989).


\textsuperscript{54} See, e.g., DoDD 5525.5, supra note 30, at 18, § E4.1.7.2.

\textsuperscript{55} See id. at 2, § 4.

\textsuperscript{56} Id. at 13–15, § E4.1.2.

\textsuperscript{57} Id. at 15–16, § E4.1.3.

\textsuperscript{58} Id. at 13, § E4.1.2.1.
a law enforcement function. OLC has since retracted in part its conclusions in this regard, and
the 10/23/01 Memorandum was criticized in the relevant retraction memorandum for being
overbroad and “divorced from specific facts.” However, while the retraction cautioned against
reliance “in any respect” on the 10/23/01 Memorandum, it also accepted the general validity of
the military purpose doctrine.

In keeping with the military purpose doctrine and in the spirit of the federal property
exception to the Posse Comitatus Act, DoDD 5525.5 exempts from Posse Comitatus
restrictions measures taken to protect Department of Defense personnel and equipment, and to
defend federal property where non-military authorities are unable to do so. This is highly
significant within the cybersecurity context, as so much activity in the field revolves around the
protection of physical governmental assets, including network infrastructure. For example,
involvelement of covered personnel at the National Security Agency in the EINSTEIN 3 private
network surveillance program, an eventuality explicitly provided for in the description of
EINSTEIN 3 given by the Comprehensive National Cybersecurity Initiative, would be

59 Memorandum from John C. Yoo, Deputy Assistant Attorney Gen., Office of Legal Counsel,
and Robert J. Delahunty, Special Counsel, Office of Legal Counsel, to Alberto R. Gonzales,
Counsel to the President, and William J. Haynes, II, General Counsel, Dep’t of Def., Authority
for Use of Military Force To Combat Terrorist Activities Within the United States 16–18 (Oct.
23, 2001) [hereinafter “10/23/01 Memorandum”].
60 Memorandum to file of Steven G. Bradbury, Principal Deputy Assistant Attorney General,
Office of Legal Counsel, October 23, 2001 OLC Opinion Addressing the Domestic Use of
Military Force to Combat Terrorist Activities 1–2 (Oct. 6, 2008).
61 Id. at 2 (“the ‘military purpose’ doctrine is a well-established limitation on the applicability of
the Posse Comitatus Act”).
62 See supra note 32 and accompanying text.
63 DoDD 5525.5, supra note 30, at 13, § E4.1.2.1.5.
64 Id. at 14, § E4.1.2.3.2.
65 For a discussion as to which personnel at NSA are subject to Posse Comitatus, see Section III,
infra.
66 NATIONAL SECURITY COUNCIL, COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE 3
(2010).
presumptively valid for Posse Comitatus purposes,\textsuperscript{67} despite potentially subjecting civilians to what might be considered “regulatory, prescriptive, or compulsory” actions, as its object is the protection of federal property in the form of networks.

On the other hand, actions such as performing arrests, searches and seizures, and interdictions for non-exempted purposes—archetypal law enforcement functions, in other words—are specifically restricted.\textsuperscript{68} Thus, although covered personnel could participate in the defense of federal networks against an attack, they would probably not be able to participate in the apprehension of the persons behind that attack, or in searches and seizures related to the investigation of the attack, once the threat to Department of Defense personnel and equipment passes.

Note, though, that Posse Comitatus only applies to a specific segment of government employees. DoDD 5525.5 applies primarily to active duty military personnel. Reservists, members of the National Guard not serving in a federalized capacity, and off-duty military personnel are not subject to DoDD 5525.5 restrictions.\textsuperscript{69} Civilian employees of the Department of Defense are similarly exempt, except where they are under the direct command and control of a military officer.\textsuperscript{70} The standard for determining command and control is eventual “accountability” to a military officer as opposed to a civilian official, even where the direct chain of command operating over a given civilian employee is entirely civilian.\textsuperscript{71}

\textsuperscript{67} Provided that civilian authorities were incapable of filling the role of the covered NSA personnel in question, pursuant to 32 C.F.R. § 215.4(c)(1)(ii).

\textsuperscript{68} DoDD 5525.5, \textit{supra} note 30, at 15, § E4.1.3.1–4.

\textsuperscript{69} \textit{Id.} at 19, § E4.2.

\textsuperscript{70} \textit{Id.} at 19, § E4.2.3.

\textsuperscript{71} See United States v. Chon, 210 F.3d 990, 993–94 (9th Cir. 2000) (finding civilian Naval Criminal Investigative Service (NCIS) personnel to be subject to Posse Comitatus restrictions as a result of the NCIS Director’s reporting relationship to the Chief of Naval Operations—a military officer).
Perhaps most significantly, DoDD 5525.5 explicitly allows for regulatory exceptions to its regime. As suggested by the language of the Act itself, Posse Comitatus restrictions only apply where Congress has not authorized actions to the contrary.72 DoDD 5525.5 carries forward the same principle, and allows for the Secretary of Defense to similarly except activities from the DoDD 5525.5 regulatory scheme.73

Having defined what Posse Comitatus does and does not require, this paper will now turn to addressing the Posse Comitatus implications of specific issues in cybersecurity policy: the creation of Cyber Command, military protection of private networks, offensive cyber operations in the homeland, and the implications of cybersecurity legislation now pending in Congress,

III. U.S. CYBER COMMAND

Secretary of Defense Robert Gates announced the establishment of U.S. Cyber Command on June 23, 2009, citing a need to deal with “a growing array of cyber threats and vulnerabilities . . . .”74 Cyber Command is to be organized as a subordinate unified command75 under the auspices of U.S. Strategic Command, one of ten current Unified Combatant Commands operating pursuant to the 2008 version of the Department of Defense’s Unified Command Plan.76 Cyber Command is to be collocated with, and will presumably draw most of its manpower from,

73 See, e.g., DoDD 5525.5, supra note 30, at 19, § 4.3.2.
75 Id.
76 The Unified Command Plan itself is classified. The Department of Defense has made available the basic parameters of the plan, though, on its website. DefenseLINK-Unified Command Plan, http://www.defense.gov/specials/unifiedcommand/.
the National Security Agency,\textsuperscript{77} while the Army’s Network Enterprise Technology Command, the Navy’s newly-reestablished Tenth Fleet, and the 24th Air Force are all expected to supply personnel as well.\textsuperscript{78} Although Cyber Command was set to be launched last October, with a projection of full operational capacity by October 2010, Congressional intransigence and concerns over privacy have delayed this process fairly substantially.\textsuperscript{79} Recently, after appearing before the Senate Committee on Armed Services,\textsuperscript{80} NSA Director Gen. Keith Alexander was finally confirmed by voice vote in the Senate to head Cyber Command.\textsuperscript{81}

Cyber Command will supplant a number of existing Strategic Command functional components, namely the Joint Task Force-Global Network Operations (JTF-GNO), and the Joint Functional Component Command-Network Warfare (JFCC-NW). The latter of these is currently based at Fort Meade, and is headed by the Director of the NSA,\textsuperscript{82} but differs from Cyber Command in terms of the breadth of its mission—JFCC-NW deals only with offensive operations, as opposed to broader-spectrum network protection and cyber supremacy.\textsuperscript{83}

Cyber Command is charged with securing “freedom of action in cyberspace” for the U.S. military, with mitigating risk related to military dependence on cyberspace instrumentalities, and

\textsuperscript{77} See Winnefeld & Alexander Hearing, supra note 4, at 28; Aaron C. Davis, Md. seen as host for new industry; State can be national center for cybersecurity, governor says, WASH. POST, Jan. 12, 2010, at B2.

\textsuperscript{78} William J. Lynn, III, Deputy Secretary of Defense, Remarks at the USAF-Tufts-Institute for Foreign Policy Analysis Conferences (Jan. 21, 2010).


\textsuperscript{80} Winnefeld & Alexander Hearing, supra note 4.

\textsuperscript{81} See Ellen Nakashima, NSA director confirmed to head cyber-command, WASH. POST, May 11, 2010, at A13.

\textsuperscript{82} See Winnefeld & Alexander Hearing, supra note 4, at 28.

with “synchronizing warfighting effects.” As a secondary matter, Cyber Command is to have the capability to provide support to “civil authorities and international partners.” The establishment of Cyber Command should not be viewed as creating any legitimately new capability for the U.S. military. Rather, it is a consolidation of existing capabilities and units into a single chain of command, which parallels the way other similar components of military power are organized within the Department of Defense.

It is this latter point, the organizational parallel, that proves most troublesome from a Posse Comitatus standpoint. Under DoDD 5525.5, employees of the National Security Agency (NSA) as a general matter would not be subject to Posse Comitatus restrictions by virtue only of their being NSA employees. Where civilian employees are not under the direct command and control of a military chain of command, Posse Comitatus restrictions on rendering aid to law enforcement do not apply. The Director of the NSA is currently an O-10 grade Title 10 military officer. This might give rise to the argument that the entire NSA should be subject to Posse Comitatus restrictions as it falls under the command and control of a military officer.

---

85 Id; see also Winnefeld & Alexander Hearing, supra note 4, at 18 (testimony of Lt. Gen. Alexander) (“Our responsibility [in the context of defending the .gov] is to provide technical support to the Department of Homeland Security. We do that under the [Comprehensive National Cyber Initiative] to help them build the technology that they need to defend those networks.”).
87 See generally DEP’T OF DEF. DIRECTIVE NO. 5158.04, UNITED STATES TRANSPORTATION COMMAND (USTRANSCOM) (2007) (designating the responsibilities and basic organization of one of the “functional” Unified Combatant Commands).
88 DoDD 5525.5, supra note 30, at 19, § E4.2.3.
89 See Winnefeld & Alexander Hearing, supra note 4, at 2–3 (identifying Lt. Gen. Alexander as Director of the NSA); Ellen Nakashima, NSA director confirmed to head cyber-command, WASH. POST, May 11, 2010, at A13 (indicating that Director Alexander had been promoted to general).
within the meaning of DoDD 5525.5 § E4.2.3. This would be a mistaken reading of precedent, of the situation, and of the relevant chain of command.

The closest case on point is *Chon*—the case involving Naval Criminal Investigative Services (NCIS) personnel cited above. In that case, the fact that the NCIS ultimately reported to the Chief of Naval Operations was considered dispositive—NCIS, despite being a civilian entity, was within the ultimate chain of command of the Navy, and was therefore bound by Posse Comitatus as made applicable by DoDD 5525.5. This case presents an almost inverse situation. Gen. Keith Alexander is the current Director of the NSA. His rank is derived from his career in the Army, a “Military Service” for the purposes of DoDD 5525.5. That having been said, he is not, as Director of the NSA, serving in his capacity as an officer in the Army, in that he does not report up the Army’s chain of command. Rather, in his capacity as head of a DoD Intelligence Component, he reports to the Secretary of Defense, at times through intermediaries such as the Under Secretary of Defense for Intelligence, and to the Director of National

---

90 See *supra*, note 71. United States v. Chon, 210 F.3d 990 (9th Cir. 2000).
91 *Id.* at 993–95.
92 DoDD 5525.5, *supra* note 30, at 1, § 2.1 (“The term ‘Military Service,’ as used herein, refers to the Army, Navy, Air Force, and Marine Corps.”).
Intelligence as the head of a member-agency of the intelligence community. The Secretary of Defense, the Under Secretary of Defense for Intelligence, and the Director of National Intelligence are civilians, and not officers of a military service within the meaning of DoDD 5525.5. If the dispositive fact in *Chon* was that the official with ultimate responsibility for NCIS’s actions was a military service officer, presumably the fact that the opposite is the case here would similarly control the matter.

Furthermore, arguing that the NSA as an entity is subject to Posse Comitatus on the ground that its director is a Title 10 military officer would mesh poorly with well-established areas of current practice. For example, Judge Advocates from the various Title 10 services often serve in a civilian capacity in the Department of Justice as Special Assistant U.S. Attorneys. In an opinion written by then-Deputy Assistant Attorney General Samuel Alito, the Office of Legal Counsel advised that these Judge Advocates, so long as they were working in a civilian capacity under a civilian chain of command, were despite their active duty status not subject to Posse Comitatus Act restrictions. The Director of the NSA is similarly working in a civilian capacity despite his rank and station in the Title 10 military. He should therefore not be considered subject to Posse Comitatus in his capacity as Director, and the agency, as it currently operates, should also fall outside of the catchment area of Posse Comitatus law.

That having been said, NSA personnel currently detailed to JFCC-NW and JTF-GNO are subject to Posse Comitatus restrictions under DoDD 5525.5 and *Chon*. JFCC-NW and JTF-GNO are both sub-components of Strategic Command, a unified combatant command operating under the Unified Command Plan and 10 U.S.C. §§ 161–68 more generally. As civilian

---

96 See DoDD 5525.5, *supra* note 30, at 1, § 2.1.
personnel detailed to the direct command and control of a military officer,\textsuperscript{98} and, more importantly under the \textit{Chon} standard, to the direct command and control of a military chain of command,\textsuperscript{99} JFCC-NW and JTF-GNO personnel fall under the exception to the civilian employee exception in DoDD 5525.5.

The advent of Cyber Command has the potential to increase the level of Posse Comitatus scrutiny that will apply to cybersecurity operations. Cyber Command is to operate as a sub-command of Strategic Command, which is a unified combatant command currently led by an Air Force general.\textsuperscript{100} As subject to the command and control of Strategic Command, any civilian Defense Department personnel detailed to Cyber Command will be subject to the Posse Comitatus Act. While many of these personnel are likely to be drawn from JFCC-NW and JTF-GNO—bodies that are already subject to Posse Comitatus restrictions—the 2010 Quadrennial Defense Review implies that Cyber Command will have farther-reaching goals than its principal precursors.\textsuperscript{101} In addition to JFCC-NW’s and JTF-GNO’s core competencies, for example, the 2010 QDR provides for Cyber Command to “direct the operation . . . of DoD’s information networks.”\textsuperscript{102} It therefore logically follows that it will draw more personnel, in the form of new hires to government service, as well as personnel from a variety of sources within the government.

The increased degree of collocation between Cyber Command and the NSA is also potentially troublesome. While JFCC-NW already operates out of Fort Meade with the NSA,\

\textsuperscript{98} DoDD 5525.5, \textit{supra} note 30, at 19, § E4.2.3.
\textsuperscript{99} \textit{Chon}, 210 F.3d at 993–95.
\textsuperscript{101} See, \textit{e.g.}, \textsc{Department of Defense, Quadrennial Defense Review Report} 38 (2010) (calling on \textsc{Cybercom} to “organize and standardize cyber practices and operations”).
\textsuperscript{102} \textit{Id}.
JTF-GNO does not. With more roles and a greater portion of the whole cyber picture being run out of Fort Meade, it is a natural possibility that non-Cyber Command NSA personnel may become entwined with Cyber Command. To the degree that these personnel may currently be engaged in activities that would be restricted under Posse Comitatus were they subject to a military chain of command, electronic searches in cooperation with civilian law enforcement for instance, their entwinement with Cyber Command has the potential to create legal problems down the road—if the NSA becomes in effect a wholly-owned outpost of Strategic Command, or if a greater proportion of NSA personnel begin spending at least some time working for Cyber Command, Posse Comitatus exemptions for NSA personnel may be more difficult to justify should they be challenged in court. It is worth noting, in relation to this issue, that part time work with both covered and non-covered entities in other contexts has previously been viewed as problematic from a Posse Comitatus standpoint by OLC.

To summarize, the standing up of Cyber Command, while causing something of a re-shuffle in the cybersecurity world, is unlikely to have major, immediate Posse Comitatus implications. While forces assigned to Cyber Command will be subject to the Posse Comitatus legal framework, most will have been already subject. However, a major risk does exist in the form of an erosion of the firewall between the NSA and uniformed chains of command, which has the potential to subject the NSA as a whole to Posse Comitatus scrutiny, which would otherwise not have been warranted.

IV. Military Protection of Private Networks

---

As the federal government seeks to put itself on sounder footing with regard to cyber-vulnerabilities, one of the emerging elements of policy that has attracted the most attention is an increased role for the government actively seeking to make secure, or causing to be made secure, private networks—either in order to help prevent a devastating attack on critical infrastructure, to build a buttress of sorts against the compromising of military and government networks, or to protect private networks for their own sake. Were Department of Defense assets to be tasked to the protection of private networks, especially over the objection of the owners of those networks, Posse Comitatus law would be implicated.

As an initial matter, actions taken to defend Department of Defense networks are not restricted by Posse Comitatus—protection of Department of Defense property is an explicit regulatory exception to the general prohibition on direct military assistance to civilian authorities. Thus, although actions taken in defense of a military network might subject civilians to “regulatory, prescriptive, or compulsory” military power, these actions would not be wrongful under Posse Comitatus.

A similar rationale is unavailable for the defense of domestic private networks. While protecting Department of Defense property is an explicitly defined exception, protection of private property does not, as a general matter, similarly allow military force to be used against civilians. Relying on Department of Defense services or agencies to provide security for private networks is thus inadvisable, barring the creation of a new statutory or regulatory exception to

107 See CENTER FOR A NEW AMERICAN SECURITY, CONTESTED COMMONS: THE FUTURE OF AMERICAN POWER IN A MULTIPOLAR WORLD 167 (2009)
108 See DoDD 5525.5, supra note 30, at 16, § E4.1.6; supra note 32 and accompanying text.
109 Id. at 18, § E4.1.7.2.
Posse Comitatus.

That having been said, there are a number of areas under the broad heading of private network security in which existing Posse Comitatus exceptions can be seen to apply. Actions taken, for example, “to prevent loss of life or wanton destruction of property” in times in which emergency authority has been invoked count as permissible direct assistance, and thus do not run afoul of Posse Comitatus law.\textsuperscript{110} Actions taken to protect classified military information are similarly permissible under Posse Comitatus\textsuperscript{111}—in the case of private networks, this would seemingly give covered Department of Defense personnel the power to take otherwise prohibited actions aimed at securing networks on which classified military information is stored without facing Posse Comitatus scrutiny. Given the prominence as an issue of cyber-espionage aimed at defense contractors, last year’s theft of F-35 fighter jet data from Lockheed most notably,\textsuperscript{112} this carve-out is not an insignificant one. Cyber Command could take steps to secure defense contractors’ networks without violating Posse Comitatus if doing so were deemed necessary to protect classified military information, presumably even over those contractors’ objections.

Similarly, there is a statutory exception to Posse Comitatus in cases of military assistance to civilian law enforcement in dealing with crimes involving nuclear materials.\textsuperscript{113} This means, for example, that the Department of Defense could, using covered personnel, take steps to secure the networks at nuclear power plants. However, because there needs to be a cognizable crime for this exception to come into effect,\textsuperscript{114} the military would have to show or be shown evidence of a forthcoming attempted attack on, or an existing conspiracy to attack, the network of the nuclear

\textsuperscript{110} DoDD 5525.5, \textit{supra} note 30, at 14, § E4.1.2.3
\textsuperscript{111} \textit{Id.} at 13, § E4.1.2.1.4.
\textsuperscript{113} DoDD 5525.5, \textit{supra} note 30, at 15, § E4.1.2.5.5.
\textsuperscript{114} \textit{Id.} (“[a]ssistance in the case of crimes”).
plant in question before it could take steps to militarily secure the network.

In summary, military intervention in the protection of private networks presumptively draws Posse Comitatus scrutiny, as it falls outside of the federal property exception. However, even under existing law, significant and relevant sub-categories of this broad class of activity are already exempted from Posse Comitatus restrictions, including actions taken to secure classified information, and actions taken to protect nuclear facilities under certain circumstances.

V: Offensive Cyber-Operations

The offensive component of cybersecurity has in recent months been at the forefront of cybersecurity discussions. At his recent confirmation hearing before the Senate Committee on Armed Services, for example, then-Lt. Gen. Alexander testified that, “In many of our war games, in many of our exercises, we noted that the offense always had the upper hand.”\footnote{Winnefeld & Alexander Hearing, supra note 4, at 21.} While JFCC-NW historically kept a very low media profile,\footnote{See John Lasker, U.S. Military’s Elite Hacker Crew, WIRED, Apr. 18, 2005.} since the announcement of the formation of Cyber Command it has not only adopted a higher profile but also has had its offensive capabilities subjected to at least cursory assessment.\footnote{See, e.g., John Markoff, David E. Sanger, & Thom Shanker, In Digital Combat, U.S. Finds No Easy Deterrent, N.Y. TIMES, Jan. 26, 2010, at A1; Ellen Nakashima, Questions stall Pentagon computer defenses, WASH. POST, Jan. 3, 2010, at A4.} The underlying concept behind offensive cyber-operations is that asymmetrical leverage inherent to cyberspace weighs the battlefield in an attacker’s favor, and will eventually cause a country seeking exclusively to defend itself to engage in highly inefficient and counterproductive spending practices.\footnote{See CENTER FOR A NEW AMERICAN SECURITY, CONTESTED COMMONS: THE FUTURE OF AMERICAN POWER IN A MULTIPOLAR WORLD 148 (2009).} In contrast, developing an offensive cyberwarfare capability allows for, assuming away the attribution dilemma, a cheaper and easier way of structuring operations, and one that has the potential to head-off future
attacks. Problematically, the Posse Comitatus Act bears against the domestic use of offensive cyber by covered Department of Defense personnel.\textsuperscript{119}

Offensive cyber-operations in the homeland will by their nature almost certainly qualify as “regulatory, prescriptive, or compulsory,”\textsuperscript{120} thus rendering them off-limits as a domestic tool to Department of Defense personnel covered by Posse Comitatus, except where the activities fall into one of the exception areas of Posse Comitatus and DoDD 5525.5. These exception areas, though, are rather difficult to apply within the context of offensive operations—it is clear, for example, that the NSA can block attacks against military networks pursuant to the federal property exemption,\textsuperscript{121} but can it do so before the attacks on our military networks even start? Does the discovery that a domestically based computer is a “zombie” justify offensive operations against it, even if it has not yet actually launched any attacks? The Posse Comitatus issues these questions raise have never been spoken to by the courts. It does appear, though, that regardless of however other laws and regulations bear on the issue, a strict reading of DoDD 5525.5 yields a fairly favorable result for those who would support an aggressive program of offensive cyber-operations.

5525.5 § E4.1.2.1 provides that “[a]ctions that are taken [by covered personnel] for the primary purpose of furthering a military or foreign affairs function of the United States” are permissible direct assistance.\textsuperscript{122} Examples of actions that qualify are enumerated,\textsuperscript{123} and include the protection of equipment and protection of classified information provisions discussed

\textsuperscript{119} Note, though, that the Posse Comitatus Act does not, as a general matter, apply extraterritorially. See 13 Op. Off. Legal Counsel 321. Offensive cyber operations conducted against targets abroad are in no way restricted by Posse Comitatus. Only offensive operations against domestic targets would have the potential to fall afoul of this area of the law.

\textsuperscript{120} DoDD 5525.5, supra note 30, at 18, § E4.1.7.2.

\textsuperscript{121} See supra note 33 and accompanying text.

\textsuperscript{122} Id. at 13, § E4.1.2.1.

\textsuperscript{123} Id. at 13, § E4.1.2.1.1–6.
previously. The words that are dispositive, though, are “[a]ctions that are taken for the primary purpose”—the question is not about what the actions are, but rather what the motivations behind them are. Following this model, it seems clear that Cyber Command cannot launch a cyber attack aimed at gathering evidence against a common criminal at the behest of local police forces. It also seems clear, though, that where covered military personnel are acting in their primary capacity as military defenders of the United States, they can launch offensive cyber attacks, so long as those attacks are not an attempt to encroach on law enforcement prerogatives. In other words, if the attack is motivated by national security rather than law enforcement concerns, then it is, at least under Posse Comitatus, allowable. This argument would appear especially true in cases where attribution, and thus a conventional law enforcement response, are difficult or impossible. Attacking systems under the control of an unknown user in an undisclosed location because of the threat posed by those systems does not look at all like the participation in civil law enforcement that the Posse Comitatus Act is set up to prevent, even if that unknown attacker ends up being domestically-based.

To summarize, offensive cyber operations are likely to be generally subject to Posse Comitatus restrictions. However, it seems reasonable that the “primary purpose” test at the heart of DoDD 5525.5’s system of regulating military interaction with civilian law enforcement will exempt broad classes of activities in this area in which the military would want to engage, and in which it is likely to engage. Posse Comitatus, in other words, should be seen as a limit on these activities, rather than as a comprehensive ban against them.

VI. CYBERSECURITY LEGISLATION

124 See supra notes 109–11 and accompanying text.
125 DoDD 5525.5, supra note 30, at 13, § E4.1.2.1.
126 This would be as close to an archetypal violation of the Posse Comitatus Act in the cybersecurity realm as the author can imagine.
There are currently four cybersecurity-related bills that have been introduced in the Senate, and the recent passage in the House of H.R. 4061 has added another to that tally. For the most part, these do not impact Posse Comitatus in any significant way. S. 778, for example, establishes an Executive Office of the President-based Office of the National Cybersecurity Adviser, and does little else. S. 1438 requires the Secretary of State to issue a report describing how the United States is working with other nations on cybersecurity—a requirement with no Posse Comitatus implications. The U.S. ICE Act, S. 921, is mostly concerned with standard setting and monitoring, and the creation of an Executive Office-based “National Office for Cyberspace.” It does not appear to implicate Posse Comitatus in any significant way. Similarly, H.R. 4061 deals with increasing funding for cybersecurity research, and would have little Posse Comitatus impact. The bill that would have the most important Posse Comitatus implications if passed is the so-called “Rockefeller Bill”—the Cybersecurity Act of 2009.

The Cybersecurity Act of 2009, co-sponsored by Senators John D. Rockefeller IV and Olympia Snowe, would, if passed, dramatically change the role of the federal government in

---

127 S. 773, 111th Cong. (2009); S. 778, 111th Cong. (2009); S. 921, 111th Cong. (2009); S. 1438, 111th Cong. (2010). Of these four, S. 773 and S. 778 are both sponsored by Sen. Rockefeller. S. 921 can be seen as a rival to the Rockefeller bills, as they cover similar ground, and seem to be supported by different interest groups. See Alexander B. Howard, ICE Act would restructure cybersecurity rule, create White House post, SEARCHCOMPLIANCE.COM, Apr. 27, 2009.
130 See S. 1438, 111th Cong. (2010).
133 S. 773, 111th Cong. (2009).
134 Id.
135 Id. at 1.
the cybersecurity realm.\footnote{See generally Joby Warrick & Walter Pincus, \textit{Senate Legislation Would Federalize Cybersecurity; Rules for Private Networks Also Proposed}, \textit{WASH. POST}, Apr. 1, 2009, at A4.} Providing for federal standard-setting with regard to the security of private networks,\footnote{S. 773, 111th Cong. (2009), at 17.} a “clearing-house” role for the federal government in cyber-threat identification and assessment,\footnote{Id. at 39.} and measures designed to encourage the development of cyber-expertise in academia and the private sector more generally,\footnote{E.g. id. at 23–31} among others, the Rockefeller Bill would represent a far-reaching overhaul of federal cyber policy with serious implications for all departments and agencies of the federal government, as well as for the private sector. Although the bill largely addresses civilian-side reforms, it does impact defense policy in a number of ways likely to implicate Posse Comitatus principles not insignificantly.

First, Section 16 of the bill provides for a “comprehensive review of the Federal statutory and legal framework applicable to cyber-related activities in the United States.”\footnote{Id. at 42.} Although the Posse Comitatus Act is not included in the short list of acts specifically marked for review,\footnote{Cf. id at 42, § 16(a)(1)–(6).} it would almost assuredly fall within a catchall provision, which covers “any other Federal law bearing upon cyber-related activities.”\footnote{Id. at 42, § 16(a)(7).} The Posse Comitatus Act dictates the way in which military personnel relate to civilian governmental instrumentalities; since the Rockefeller Bill does attach a great deal of importance to governmental coordination,\footnote{See, e.g., id. at 18, § 6(a)(5) (calling for the development of Government-wide security setting configurations).} it would be difficult to see how Posse Comitatus would not fall within the Bill’s ambit. Additionally, DoDD 5525.5 and other orders and regulations that relate to Posse Comitatus would fall within another catchall:
“any applicable Executive order or agency rule, regulation, guideline.” Since DoDD 5525.5 dictates the way military personnel would have to act in response to some cybersecurity issues, labeling it “inapplicable” for the purposes of the act would be difficult.

Another element of the Rockefeller Bill, Section 14, empowers the Department of Commerce to serve as a clearinghouse for cyber-threat and vulnerability information. It further states that the Secretary of Commerce’s access to information relevant to that role shall be granted “without regard to any provision of law, regulation, rule, or policy restricting such access . . . .” This provision should rightfully be considered a statutory exception to Posse Comitatus. DoDD 5525.5 explicitly prohibits the sharing of information by Military Departments and Defense Agencies with civilian authorities where doing so would “adversely affect . . . military preparedness.” In the cybersecurity context, it is possible, for example, that sharing information about a particular software vulnerability with the Commerce Department could increase the profile of that vulnerability, and, if military systems were to remain un-patched, that this information sharing could end up harming military preparedness. Regardless of the propriety of this sort of information hoarding, DoDD 5525.5 would currently allow for it, while the Rockefeller Bill would explicitly forbid the withholding of any such information because of contrary positive law or regulation.

The final component of the Rockefeller Bill that raises Posse Comitatus questions relates to the proposed new powers of the President to respond to cybersecurity emergencies. Section

\[144\] Id. at 42, § 16(a)(8).
\[145\] Use of covered personnel to surveil suspected, domestically-based cyber-attackers, for example. See DoDD 5525.5, supra note 30, at 16, § E4.1.3.4.
\[146\] DoDD 5525.5, supra note 30, at 9, § E2.2.
\[147\] See S. 773, 111th Cong. (2009), at 39, § 14(b)(1).
18(2) allows the President to declare a cybersecurity emergency,\(^{148}\) and Section 18(3) charges him with “designat[ing] an agency to be responsible for coordinating the response” to the emergency he has declared.\(^{149}\) This language gives the President a great degree of latitude in determining how best to respond to attacks on our critical infrastructure, but also implicates Posse Comitatus issues. If the President were, for example, to choose a military component as his lead agency (this might not be unreasonable depending on what “response” is warranted by the emergency in question, and given the role envisioned for Cyber Command), that might subject all Defense Department personnel “responding” to the emergency to Posse Comitatus rules (they would be operating under a military chain of command).\(^{150}\) If they were to violate Posse Comitatus, such issues as the possibility of the application of an exclusionary rule to any evidence they gather in the process rise to the fore.\(^{151}\) Alternatively, if the president were to select a civilian agency as his lead, military departments and defense agencies might be constrained by DoDD 5525.5 in terms of the sort of information they could share,\(^{152}\) as was discussed in the context of Section 14 above.\(^{153}\)

In short, although it is not primarily addressed at Defense-sector entities, the Rockefeller Bill does have some Posse Comitatus Act implications, and would in fact mandate a statutory and regulatory review of the existing Posse Comitatus legal regime. While that is not in and of itself a bad thing, it does appear to be an unintended and unconsidered second-order effect of the bill, and therefore perhaps deserves more attention as the legislative process proceeds.

\(^{148}\) Id. at 44, § 18(2).

\(^{149}\) Id. at 44, § 18(3).

\(^{150}\) See DoDD 5525.5, supra note 30, at 19, § E4.2.3.

\(^{151}\) See United States v. Wolffs, 594 F.2d 77, 85 (5th Cir. 1979) (stating that were a pattern of “widespread and repeated violations of the Posse Comitatus Act” to be uncovered, application of an exclusionary rule would be appropriate).

\(^{152}\) See DoDD 5525.5, supra note 30, at 9, § E2.2 (military preparedness exception).

\(^{153}\) See supra p. 26.
VII. CONCLUSION

The Posse Comitatus Act has been described as dated and anachronistic, and a cursory search of the scholarship that deals with it yields a mass of proposals to scrap or redesign it in various ways with equally varied likely results.\textsuperscript{154} Even so, the Posse Comitatus Act, and its accompanying body of legislation and regulation, has proven remarkably resilient, and remains the law—and until it is either severely eviscerated by statutory exceptions or overturned in its entirety it will remain the law. As such, it is worth noting what it does and does not allow military personnel to do.

The fact that organizational structures for and doctrinal approaches to cybersecurity are so new, and developing so rapidly, gives further impetus to the study of the Posse Comitatus Act. The creation of Cyber Command and the puzzle resulting from its amalgamation of military and civilian personnel form something of a case study in the complexities of departmental and functional governmental reorganization efforts.

It is likely that, as it functions as a set of default rules, the Posse Comitatus Act will be subjected to the indignity of further accidental amendments, and that it will impact newly formed legal structures, even if only tangentially. The Rockefeller Bill, and the fairly serious Posse Comitatus implications resulting from it, which were almost certainly unintentional, demonstrates both of these phenomena quite clearly.

As cybersecurity policy becomes more definite in coming years, and as approaches like governmental involvement in the defense of private networks and the use of offensive cyber as a

supplement to traditional network defense become more well-established, questions will continue to emerge around the underlying problem of where to draw the line—what constitutes illegal use of the military for domestic law enforcement, and what constitutes proper use of the military for defense. It may, in the end, be time for a new statutory exemption to the Posse Comitatus Act, exempting forces assigned to Cyber Command from its strictures, or specifically allowing for the use of the military in matters related to elements of cybersecurity activity. Whether such an approach is taken or not, though, the Posse Comitatus Act and the principle for which it stands, that Americans should not be subjected to the power of their own military in the domestic law enforcement concept, will continue to play a role in debates over the proper form of governmental action in this area for many years to come.