Journal of International and Comparative Law

Volume 4, Fall 2013, Issue 1 Article 2

Cyberthreats and the Posse Comitatus Act: Speculations

Susan W. Brenner

CYBERTHREATS AND THE POSSE COMITATUS ACT: SPECULATIONS

*Susan W. Brenner**

INTRODUCTION

As I have explained elsewhere, cyberthreats – cybercrime, cyberterrorism and cyberwarfare – create new challenges for nation-states because they do not conform to the essentially dichotomous threat model that has evolved over the last few centuries.[1] Every human social system must maintain a baseline of order if it is to survive and prosper.[2] Order is essential if the individuals who comprise such a system are to carry out the tasks that are essential for their survival and for the consequent survival of that social system.[3]

Threats to order come both from the "inside" and the "outside."[4] "Outside" threats – acts of war – come from other social systems, e.g., other nation-states.[5] Individuals, of course, conduct war, but in so doing they act on behalf of their sovereign; they are basically the instruments states use to challenge the viability of another state.[6]

"Inside" threats come from within a system, where citizens prey on other citizens in various ways. Since humans are individually intelligent, they can choose not to follow the rules that otherwise ensure internal order, i.e., they can commit crimes or acts of terrorism.[7] Unless societies develop techniques that control such activity, crime and/or terrorism will threaten the stability of a social system.[8]

---

* Samuel A. McCray Chair in Law, University of Dayton School of Law.

[1] *See, e.g.*, Susan W. Brenner, *Toward A Criminal Law for Cyberspace: Distributed Security*, 10 B.U. J. SCI. & TECH. L. 1, 65 (2004); *see also* SUSAN W. BRENNER, CYBERTHREATS: THE EMERGING FAULT LINES OF THE NATION-STATE 29 (2009).

[2] *See, e.g.*, Brenner, *Toward A Criminal Law for Cyberspace: Distributed Security, supra* note 1, at 9.

[3] *See id.*

[4] *See id.* at 10−11.

[5] *See, e.g.*, Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379, 402 (2007).

[6] *See id.* at 402−03.

[7] *See* Brenner, *Toward A Criminal Law for Cyberspace: Distributed Security, supra* note 1, at 35.

[8] *See id.* at 45−46.

The next section reviews how Anglo-American societies have dealt with the need to control both types of threats and thereby ensure the order necessary for a society to survive.

I. The Militia, the Posse Comitatus and the Posse Comitatus Act

The militia and the posse comitatus evolved in Anglo-Saxon England and were brought to what would become the United States by the British colonists.[9] In Anglo-Saxon times, and for centuries thereafter, Britain did not have either a standing army or a professional police force.[10] Instead, it relied on two *ad hoc* entities, both of which were composed of the able-bodied men of the community, who were required to be armed and prepared to use those arms when called upon for assistance.[11]

When this *ad hoc* group was called upon to repel a foreign enemy, it was the militia; when it was called upon to apprehend criminals, it was the posse comitatus.[12] This system prevailed until into the nineteenth century.[13] It faded away as it became apparent that the militia was no match for professional soldiers, and the posse comitatus was not capable of dealing with the urban crime that emerged as the century progressed.[14]

The eventual result was that by the twentieth century the United States, along with other countries, had a bifurcated threat-control system: the military, an institution staffed by trained professionals, deals with threats from "outside," i.e., with attacks launched by other nation-states.[15] And the process of controlling internal threats – crime and terrorism – became the responsibility of professional police forces,[16] which trace their origin to Sir Robert Peel's establishment of the Metropolitan Police in

---

[9] *See, e.g.*, BRENNER, CYBERTHREATS, *supra* note 1, at 167.
[10] *See id.*; *see also* Harold S. Herd, *A Re-Examination of the Firearms Regulation Debate and Its Consequences*, 36 WASHBURN L.J. 196, 200 (1997).
[11] *See, e.g.*, Herd, *supra* note 10.
[12] *See, e.g.*, Worth v. Craven County Com'rs, 24 S.E. 778, 779 (N.C. 1896).
[13] *See, e.g.*, United States v. Miller, 307 U.S. 174, 178−79 (1939); *see also* LAWRENCE M. FRIEDMAN, CRIME AND PUNISHMENT IN AMERICAN HISTORY 29, 174 (1994).
[14] *See, e.g.*, Robert J. Spitzer, *The Second Amendment "Right to Bear Arms" and United States v. Emerson*, 77 ST. JOHN'S L. REV. 1, 5−6 (2003); *see also* Frederick Bernays Wiener, *The Militia Clause of the Constitution,* 54 HARV. L. REV. 181, 188−90 (1940). As to professional policing, *see, e.g.*, Brenner, *Toward A Criminal Law for Cyberspace: Distributed Security, supra* note 1, at 61−65.
[15] *See, e.g.*, Akhil Reed Amar, *The Second Amendment: A Case Study in Constitutional Interpretation*, 2001 UTAH L. REV. 889, 911 (2001).
[16] *See id.* ("Law enforcement has shifted to police departments").

nineteenth-century London.[17] Peel replaced the posse comitatus with a uniformed, quasi-military organization, which proved much more effective at dealing with the urban crime that increasingly plagued British cities and their American counterparts.[18] Peel's system spread to other countries, as well.[19] The result is that threat control is more or less rigidly, depending on the country in question, divided between the military (warfare) and the police (crime and terrorism).[20]

That was not always true, even after the U.S. adopted professional policing. In the years leading to the Civil War, federal marshals used troops to enforce federal law, and after the War federal troops enforced the law in the post-Civil War South.[21] As a result of perceived abuses resulting from the latter, in 1878 Congress adopted the Posse Comitatus Act "to put an end to the use of military for ordinary law enforcement purposes." [22] The Posse Comitatus Act is still in force and currently states that "[w]hoever, except in cases . . . expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force . . . to execute the laws shall be fined . . . or imprisoned not more than two years, or both."[23] While the Act explicitly applies only to the Army and Air Force, Department of Defense regulations extend its restrictions to the Navy and Marines.[24]

---

[17] *See, e.g.*, David A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165, 1202 (1999).

[18] S*ee, e.g.*, Brenner, *Toward A Criminal Law for Cyberspace: Distributed Security, supra* note 1, at 63−64. New York established a police force in 1845 and other cities followed suit. *See, e.g.*, Sklansky, *The Private Police, supra* note 17, at 1207.

[19] *See, e.g.*, CLIVE EMSLEY & BARBARA WEINBERGER, POLICING WESTERN EUROPE: POLITICS, PROFESSIONALISM AND PUBLIC ORDER 1−14, 18−24, 55−68 (Greenwood 1991).

[20] *See, e.g.*, Susan W. Brenner, *Cyberthreats and the Limits of Bureaucratic Control,* 14 MINN. J.L. SCI. & TECH. 137, 197–198, 231 (2013). After the 911 attacks, terrorism's status as an internal threat began to blur, but that is not an issue I can address here, given the brevity of this article. *See, e.g.*, Mariona Llobet, *Chapter 5 Terrorism: Limits Between Crime And War. The Fallacy Of The Slogan 'War On Terror'*, 14 IUS GENTIUM 101, 101–109 (2012).

[21] *See, e.g.*, Nathan Canestaro*, Homeland Defense: Another Nail in the Coffin for Posse Comitatus,* 12 WASH. U. J.L. & POL'Y 99, 110−11 (2003); *see also* Sean O'Hara, Comment, *The Posse Comitatus Act Applied to the Prosecution of Civilians,* 53 U. KAN. L. REV. 767, 771−72 (2005); *see also supra* note 18.

[22] *See* O'Hara*, supra* note 21, at 772 (citing Army Appropriations Act, ch. 263, §15, 20 Stat. 145, 152 (1878) (codified as amended at 18 U.S.C. § 1385 (1994))).

[23] 18 U.S.C § 1385 (1994).

[24] *See* O'Hara*, supra* note 21, at 772 (citing U.S. Dep't of Defense, Directive No. 5525.5, *amended by* No. 3025.21, DoD Cooperation with Civilian Law Enforcement Officials, encl. 4 at 4.3 (Jan. 15, 1986)).

The Posse Comitatus Act is the primary principle that bars the U.S. military from participating in civilian law enforcement.[25] As the Supreme Court noted, its unique and exclusive function is "to fight or be ready to fight wars should the occasion arise."[26]

II. Cyberthreats and the Posse Comitatus Act

This section reviews how cyberthreats undermine the viability of the threat response system examined in Section I.[27] It also analyzes whether it would be possible, and prudent, to modify the system in ways that could allow for more flexible responses to threats of both types.

A. The Problem

As noted above, the United States, like most twenty-first century nation-states, employs a bifurcated threat-response and control system which is predicated on the assumption that threats to social order are readily divisible into "inside" threats (law enforcement) and "outside" threats (the military). While this system has proven quite satisfactory in dealing with real-world threats, it breaks down as threat activity migrates "into" cyberspace, i.e., as malefactors use digital technology to attack individual or governmental targets in their own country or halfway around the world.

Cyberspace transcends spatial boundaries and thereby erodes the distinction between "inside" and "outside" threats. It can be difficult to determine whether cyberattacks came from "inside" or "outside" a particular state. And even if it is clear that an attack came from "outside," the attack may not otherwise conform to the definition of an "outside" attack, i.e., an act of war. Conversely, when an attack comes from "inside," it may not otherwise conform to the definition of an "inside" attack, i.e., it may not clearly qualify as crime or terrorism.

For example, in the spring of 2013, Mandiant, a U.S. computer security firm, issued a report that described how a specialized unit of the People's Liberation Army[28] ("PLA") was, and had for years been, hacking into computers of U.S. businesses

---

[25] *See, e.g.*, Adam Burton, *Fixing FISA for Long War: Regulating Warrantless Surveillance in the Age of Terrorism*, 4 PIERCE L. REV. 381, 389 (2006).
[26] Toth v. Quarles, 350 U.S. 11, 17 (1955).
[27] *See* BRENNER, CYBERTHREATS, *supra* note 1, at 29.
[28] *See Structure and Organization of the Armed Forces*, MINISTRY OF NATIONAL DEFENSE, THE PEOPLE'S REPUBLIC OF CHINA, http://eng.mod.gov.cn/ArmedForces/index.htm.

and stealing proprietary information.[29] Stealing proprietary information is a federal crime.[30] The PLA members who were engaging in this activity were therefore committing a crime "in" the United States, but this was not a conventional crime. Uniformed members of a nation-state's military acting on behalf of their sovereign were committing it.

That raises a number of difficult issues. For one thing, it is almost certain that China would not extradite the PLA members to the United States to be prosecuted for their crimes because China is, at the very least, complicit in those crimes.[31] The civilian law enforcement system can, as a result, do nothing to retaliate against or halt this type of activity. For another, the scenario seems to mix metaphors: since the activity that would otherwise constitute a crime was carried out by military personnel who were acting on behalf of their sovereign, does it constitute war?

Or consider a different scenario: in June of 2009, cybercriminals surreptitiously extracted $415,989 from an account at the First Federal Savings Bank in Shepherdsville, Kentucky.[32] The account belonged to Bullitt County. The transfers were not discovered until the money was gone. Officials contacted the Federal Bureau of Investigation, which determined the transfers originated in Ukraine. The thieves used a Trojan Horse program installed on the County Treasurer's computer to extract the funds.[33]

No one was, and no one will be, charged with the Bullitt County theft, which is unfortunate because online bank robbery is far from uncommon: in the spring of 2013, "hackers in Ukraine and Russia" extracted $1.3 million from a Washington hospital.[34] Since the United States does not have an extradition treaty with Russia,[35] and Ukraine is a cybercrime haven,[36] no one will be prosecuted for this crime, and, like Bullitt County, this hospital will never recover the lost funds.

---

[29] *See, e.g.*, David E. Sanger, David Barboza & Nicole Perlroth, *Chinese Army Unit Is Seen as Tied to Hacking against U.S.*, N.Y. TIMES (Feb. 18, 2013), http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all.

[30] *See* 18 U.S.C § 1831 (1996).

[31] *See* 18 U.S.C. § 3181 (1996) (The United States and China do not have an extradition treaty).

[32] *See* Brian Krebs, *PC Invader Costs Ky. County $415,000,* WASH. POST (July 2, 2009), http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html.

[33] *See id.*

[34] *See* Brian Krebs, *Wash. Hospital Hit by $1.03 Million Cyberheist*, KREBS ON SECURITY (Apr. 13, 2013), http://krebsonsecurity.com/category/smallbizvictims/.

[35] *See* 18 U.S.C. § 3181 (1996).

[36] *See, e.g.*, Yuriy Onyshkiv, *Ukraine Thrives as Cybercrime Haven*, KYIV POST (Mar. 8, 2012), http://www.kyivpost.com/content/ukraine/ukraine-thrives-as-cybercrime-haven-123965.html.

What has all this to do with the Posse Comitatus Act? It has several implications for the system of threat control upon which the United States relies. One consequence of that system is, as noted earlier, that law enforcement officers deal with "inside" threats, which logically implies that they do not pursue "outside" threats. That, of course, is not literally true, nations have developed systems in which officers from various countries can cooperate and offenders can be extradited for prosecution in the United States.[37]

The problem is that, while states have historically had an incentive to cooperate in the apprehension and prosecution of traditional criminals whose activities can threaten social order in more than one state, they may not have an incentive to cooperate when the crimes at issue are virtual and have little, if any, likelihood of negatively affecting the host country. Cybercrime can bring billions into a country, like Ukraine or Russia; while the state itself is usually not complicit in this type of activity, it still benefits from it.[38] And if the haven state's law enforcement will not cooperate with U.S. law enforcement that effectively means no one will be sanctioned for the crime(s).

If these examples seem trivial in their import, consider this: the bank theft cases illustrate the extent to which U.S. law enforcement cannot protect American citizens from external crime. The Mandiant report illustrates the extent to which neither U.S. law enforcement nor the U.S. military can protect American citizens from Chinese military personnel who are stealing their proprietary information. And to make that scenario more interesting, assume that instead of simply stealing trade secrets, the PLA members are infiltrating U.S. infrastructures, such as the power grid and financial system, in order to acquire the ability to sabotage them, in whole or in part.[39]

B. Implications for the Posse Comitatus Act?

As we saw above, the United States' threat response systems are of little utility in dealing with attacks from abroad. Law enforcement has little ability to operate in other countries, and what ability it has depends on the acquiescence and support of the government in a particular state. This is not surprising, since U.S. authorities are unlikely to acquiesce in and support the efforts of foreign law enforcement officers – Russian police, for example –

---

[37] *See, e.g.*, Gregor Urbas, *Cybercrime, Jurisdiction and Extradition: The Extended Reach of Cross-Border Law Enforcement*, 16 No. 1 J. INTERNET L. 1, 9 −13 (2012).

[38] *See, e.g.*, *Russian Hackers Get Big Slice of Cyber Crime Billions*, RT (Apr. 24, 2012), http://rt.com/business/russia-cyber-crimes-cost-860/.

[39] *See, e.g.*, Sanger, Barboza & Perlroth, *supra* note 29.

who wish to conduct an investigation in the United States that targets U.S. citizens. Law enforcement has been, and continues to be, parochial.

The military not only has the ability to operate in other countries, that is its default mission (absent an armed invasion of U.S. territory). But the military cannot participate in law enforcement, at least not under the Posse Comitatus Act.[40] While it is not clear if the Act applies extraterritorially, the Department of Defense operates on the premise that it does, subject to certain exceptions.[41] The Posse Comitatus Act, then, is the only legal principle that bars cooperation between law enforcement and the military. Nothing in the Constitution prohibits this: when the Constitution was drafted the nation's threat control system consisted of the able-bodied men of the nation, who acted as law enforcers or as members of the military, depending on the circumstances.

Logically, that approach has a certain appeal in a world in which computer and other technology erodes the import of national boundaries, especially as far as threat control is concerned. Should we reassess the Posse Comitatus Act, with an eye to modifying or repealing it? So far, I continue to be agnostic on that issue, but I think it is worth exploring to determine if there was a way to think about how we might approach threat control differently. To that end, therefore, I shall speculate about what might be involved in relaxing or eliminating the Act's prohibition on cooperation between civilian law enforcement and the military.

C. Repeal or Modify the Posse Comitatus Act

I begin with the most drastic option – eliminating the Act. Actually, I begin with what I see as two, more or less equally drastic options: one is to simply repeal the Posse Comitatus Act, thereby eliminating the prohibition on law enforcement-military collaboration. The other, somewhat less drastic option, would be to modify the Posse Comitatus Act so that it bars law enforcement-military collaboration in the physical world but not when the activity at issue involves cyberattacks.

While the notion of repealing the Posse Comitatus Act has an attractive simplicity, I cannot contemplate such a step without trepidation. As one author noted, "there is something inherently

---

[40] *See* 18 U.S.C. § 1385 (1956).

[41] *See, e.g.*, Cristian DeFrancia, *Enforcing the Nuclear Nonproliferation Regime: The Legality of Preventive Measures*, 45 VAND. J. TRANSNAT'L L. 705, 768 (2012).

repugnant to most Americans at the thought of the military patrolling the streets of our cities and towns."[42] This is not because we do not trust our military, but because we fear what it might become if we took this step. Also, we would likely gain little from repealing the Posse Comitatus Act because the military has no expertise in civilian law enforcement.[43] If we went down this path, we might actually undermine the effectiveness of the military and law enforcement by eroding the distinctiveness of their respective missions. And, finally, repealing the Act would be overkill, since the bifurcated response system seems to work quite well with regard to activity in the physical world.

That brings us to the other option – modifying the Posse Comitatus Act so it does not bar law enforcement-military collaboration with regard to activity that occurs in or is vectored through cyberspace. Since the impetus for reconsidering it is the difficulties law enforcement and the military respectively confront in dealing with cyberthreats, this would seem a more logical, more focused approach.

The question then becomes, what, precisely, would we seek to achieve by modifying the Posse Comitatus Act? Do we, for example, want our military to be able to act as law enforcement agents (or surrogates) when it is necessary to deal with cyberattacks from abroad? If the answer to that question is yes, then I have another question: what, precisely, would we want the military to do?

In both of the scenarios we examined earlier, foreign nationals were committing crimes by stealing property (funds in one case, trade secrets in the other) from American citizens who were in the United States. In one case, the perpetrators were members of the Chinese military; in the other, they were Ukrainian citizens. Unless and until we modify our conceptualization of the threat array, the activity in both instances constituted crime, rather than warfare.

It might, therefore, seem as if the U.S. military would have no conceivable role to play in responding to these and similar attacks, since I assume no rational person would argue that the United States should launch a retaliatory military strike on China (or on Ukraine) in response to these thefts. That does not necessarily mean that the U.S. military might not be able to assist law enforcement in ways that could enhance the latter's ability to respond effectively to cross-border crimes.

---

[42] *See* Dan Bennett, *The Domestic Role of the Military in America: Why Modifying or Repealing the Posse Comitatus Act Would Be a Mistake*, 10 LEWIS & CLARK L. REV. 935, 944 (2006).

[43] *See, e.g.*, *id.* at 944−45.

As we saw above, in neither case will U.S. law enforcement be able to have the perpetrators extradited so they can be charged, prosecuted and presumably convicted in the United States. Some, though, argue that law enforcement should be able to employ other measures to create at least something of a disincentive to attack Americans. They contend that U.S. law enforcement should be able to use "electronic sanctions" to react to cybercrimes.[44] Relatively recently, I discussed this issue with a former Department of Homeland Security official who, as far as I could determine, seemed to be arguing that this type of a response is lawful under Model Penal Code § 3.09(1) either to prevent the theft of "movable property" or to retake such property.

If we accept that argument, at least for the purposes of analysis, then we need to address the practicalities it presents: how is U.S. law enforcement going to use virtual force to strike back at someone attempting theft who is located in another country? I have not found any authority for this proposition, but I strongly suspect U.S. law enforcement does not have the constitution, statutory or common law authority to attack targets in another country. The military, of course, does have such authority, at least as a general matter. So *if* (and I regard that as a significant qualifier) we were to decide we want to employ online strike-back techniques as a way to create disincentives to use cyberspace to attack American targets, and *if* we made the appropriate modifications to the Posse Comitatus Act, the military could either support law enforcement's efforts in this regard or actually be responsible for carrying out the strike-back attacks.

This is but one obvious example of what allowing U.S. law enforcement and the U.S. military to collaborate in dealing with extraterritorial cybercrime might involve. I offer this scenario purely for the purposes of analysis – as a way of illustrating the possible utility of modifying the Posse Comitatus Act to allow this type of collaboration. Personally, I have serious reservations about our going down this path. Aside from anything else, I fear it could have serious consequences, i.e., that what began as a law enforcement strike-back attack could escalate until the two countries were at war with each other, on- and/or off-line.

D. Allow U.S. Law Enforcement to Support Military's Efforts in Cyberspace

The Posse Comitatus Act prohibits using the military in civilian law enforcement. It does not prohibit using law

---

[44] *See, e.g.*, Joel R. Reidenberg, *States and Internet Enforcement*, 1 U. OTTAWA L. & TECH. J. 213, 228 (2004).

enforcement to support the military's efforts to deal with attacks from other nation-states. Logically, then, we could allow U.S. law enforcement officers to support the military's efforts to deal with cyberattacks that are directed at U.S. targets and that are carried out by another nation-state (presumably by its military).

The question then becomes, what might we gain from taking this step? From the little I know about the U.S. military's preparation for cyberwar, I am quite confident they do not need any assistance in developing the appropriate weaponry or skills necessary for this endeavor. I am also assuming that law enforcement officers would add little to the military's ability to deal with cyberattacks from other states. This assumption is basically the converse of the assumption we made above, i.e., that the military can add little, if anything, to law enforcement's ability to deal with crime, including cybercrime.

There is at least one thing that law enforcement might be able to contribute to the military's efforts in this regard: threat information. Unlike conventional warfare, which is conducted in public and has traditionally been directed at military targets only, cyberattacks tend to be directed at civilian targets. Earlier, I raised the scenario in which PLA members are exploring the networks used by U.S. infrastructure providers to learn how to sabotage them.[45] Civilians, including law enforcement, have much greater access to information about activity such as this, because while there may be no statutory or constitutional prohibition on the U.S. military's monitoring U.S. civilian entities to detect possible cyberthreats, this type of activity would probably encounter opposition from the public, and their representatives.[46] While it would probably not eliminate the opposition, allowing law enforcement to share information it collected while legitimately carrying out its professional duties might significantly mitigate it.[47]

E. Create an Entirely New Entity

Another option I do not support would be to create a new entity, which was neither wholly law enforcement nor wholly military but was able to deal with threats that were purely internal, purely external, and that had elements of each. I do not favor this because I believe adding another layer of institutional bureaucracy would only further impede the nation's ability to deal effectively with cyberthreats.

---

[45] *See* Sanger, Barboza & Perlroth, *supra* note 29.
[46] *See generally* Mark D. Young, *United States Government Cybersecurity Relationships,* 8 I/S: J. L. & POL'Y FOR INFO. SOC'Y 281, 303−04 (2012).
[47] *See generally* Laird v. Tatum, 408 U.S. 1, 6−7 (1972).

F. Regress

Since cyberthreats do not fall neatly into the "inside" – "outside" threat dichotomy and consequently tend to resist the efforts of the correlate threat response systems on which we currently rely, another option would be to begin to decentralize threat response systems to place at least some responsibility for identifying and resisting threats on the civilian entities that are most likely to be targeted. The effort might eventually expand to do something similar with individual civilians, as well, but it would be more reasonable, and more feasible, to begin with corporate and other entities.

Such an effort would, in effect, involve extrapolating the common law militia and the posse comitatus into the cyber arena so that companies and other essential institutions would be charged with protecting themselves from attacks. Government entities, including law enforcement and the military, could support them in this regard, with expertise, technologies and other assets. The advantage of involving the civilian sector is that it would not only enhance the threat-detection and response capabilities of law enforcement and the military, it would also give both access to more detailed threat data than they currently have.

CONCLUSION

> *The cyberworld is so new that the old structures. . . break down. . . .*[48]

My arguments and analysis in this piece may seem simplistic, and that may be a fair assessment because it is very difficult to addresses the complexities and nuances of the issues I elected to address in a relatively short piece. My goal here is simply to point out issues that will become problematic and, as I noted earlier, speculate a bit about how we might address and resolve them. I firmly believe that the challenges cyberspace creates for those we trust to protect us of threats of whatever kind cannot be underestimated if we are to address and overcome them.

---

[48] *See* Michael Joseph Gross, *Enter the Cyber-dragon*, VANITY FAIR, Sept. 2011, at 11.