Major General Charles J. Dunlap, Jr.*

Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors

Presented at the

Air University 2008 Cyberspace Symposium

Maxwell AFB, AL

16 July 2008

Ladies and gentlemen, thank you very much for the opportunity to speak with you about the legal and, indeed, philosophical issues with which we are grappling today and will certainly grapple in the coming years. Before proceeding, let me state for the record that I am giving you my personal opinion, and not necessarily that of the U.S. government or any of its instrumentalities.

Let me begin with the observation that the cyber world in all its many dimensions is embedded in virtually all national security issues.[1] Consider that the Department of Defense ("DoD") defines cyberspace as the "global domain within the information environment

* Deputy Judge Advocate General of the United States Air Force, Pentagon, Washington, D.C.; J.D., Villanova University; B.A., St. Joseph's University (History).

1. The importance of cyberspace to our national security is recognized at the highest levels of government: "Our Nation's critical infrastructures consist of the physical and cyber assets of public and private institutions in several sectors: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is the nervous system of these infrastructures—the control system of our country. Cyberspace comprises hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security." NATIONAL STRATEGY

consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2]

Obviously, there is hardly any aspect of modern military operations that fails to involve cyberspace in some way, and much the same can be said about our economy[3] and, indeed, our way of life.

Defending our way of life is the *raison d'être* of America's armed forces.[4] This brings me, however, to my first point, and this is simply that because a particular cyber-related matter has a national security dimension does not mean, necessarily, that it is appropriate for the armed forces to address.

I believe that in the twenty-first century, national security challenges do require a national response. We need to bring all elements of national power to bear and that, by definition, requires robust involvement of agencies and entities outside the DoD. This is particularly important in the context of cyber matters. Much of what transpires in the cyber realm that concerns us does not resemble traditional military threats.[5] That is something of an issue because our legal architecture for the law of war is built upon the concept of traditional military threats.

TO SECURE CYBERSPACE vii (2003), http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

2. JOINT CHIEFS OF STAFF, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 141 (2001), http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

3. "By 2003, our economy and national security became fully dependent upon information technology and the information infrastructure. A network of networks directly supports the operation of all sectors of our economy—energy (electric power, oil and gas), transportation (rail, air, merchant marine), finance and banking, information and telecommunications, public health, emergency services, water, chemical, defense industrial base, food, agriculture, and postal and shipping. The reach of these computer networks exceeds the bounds of cyberspace. They also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, and radars." NATIONAL STRATEGY TO SECURE CYBERSPACE, *supra* note 1, at 6.

4. "The Armed Forces fulfill unique and crucial roles, defending the United States against all adversaries and serving the Nation as a bulwark and the guarantors of its security and independence. When called to action, the Armed Forces support and defend national interests worldwide." JOINT CHIEFS OF STAFF, DOCTRINE FOR THE ARMED FORCES OF THE UNITED STATES i (2007), http://www.dtic.mil/doctrine/jel/new_pubs/jp1.pdf.

5. Such cyber threats to national security can take a variety of forms: "[Small groups or individuals] can attack vulnerable points in cyberspace and disrupt commerce and daily life in the United States, causing economic damage, compromising sensitive information and materials, and interrupting critical services such as power and information networks. National security and domestic resources may be at risk . . . ." DEP'T OF DEFENSE, 2008 NATIONAL DEFENSE STRATEGY 7 (2008), http://www.defenselink.mil/pubs/2008NationalDefenseStrategy.pdf.

As I will discuss in a moment, that does not mean, however, that all the laws and treaties are irrelevant; rather, it means that it takes hard work and innovative analysis to apply existing law to emerging cyber issues.

For example, one of the central issues—a truly perennial one—is when does a specific cyber activity constitute the kind of peril that makes it appropriate for a national security response as opposed to a law enforcement response? This is not a new issue; as an aside, I wrote an article about this subject in 1996, yet here we are today still wrestling with it.[6]

I am an adherent of the "Schmitt test," which was enunciated in a 1999 law review article by Michael N. Schmitt, a retired Air Force judge advocate.[7] What he does, as many of you know, is lay out a number of factors to consider.[8] The aim of this analysis is to determine when the consequences of a particular cyber event have an effect that mirrors that of a traditional kinetic attack. If it does, the whole panoply of the law of war may apply.[9]

Sounds simple? The concept is simple, but its application is complicated because it requires subjective and qualitative judgments that, like so many judgments in the military and diplomacy realms, reside in an arena of imperfect information and grey areas.

The only solution to this is to attempt to work through various scenarios in exercises and other controlled situations so that we can develop robust ways of thinking about the criteria, and figure out the

6. Charles J. Dunlap, Jr., *Cyber Attack! Are We at War?*, J. NAT'L COMPUTER SECURITY ASS'N, Nov. 1996, at 18.

7. Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. OF TRANSNAT'L L. 885 (1999).

8. *Id.* at 935. Professor Schmitt sets forth a multi-factor test for analyzing a computer network attack under international law, with a particular view toward the United Nations Charter. His analysis turns on such questions as whether an attack is "intended to directly cause physical damage to objects or injury to human beings," "whether the consequences of the attack track those consequence commonalities which characterize armed force," and whether principles such as self-defense are applicable. *Id.* Professor Schmitt's test uses similar questions in order to evaluate the appropriateness of a response by armed force to such an attack.

9. Such considerations continue to be at issue at the highest levels of national security decision-making. *See* John T. Bennett, *Renuart: New President Faces Cyber, Arctic Threats*, DEFENSE NEWS, Aug. 20, 2008, http://www.defensenews.com/story.php?i=3684947&c=AME&s=TOP ("As the federal government continues efforts to piece together how to implement President George W. Bush's super-secret, multibillion-dollar cyber security program, Air Force Gen. Victor Renuart, U.S. Northern command chief, says success in the electronic domain will require 'a multi-nation approach.' It is difficult to determine whether an attack on a nation's cyber infrastructure is an act of war because 'we have not yet defined what that is,' Renuart said. 'That's a policy decision that has to be made. I don't think any nation is ready to make that kind of declaration . . . .'").

optimal way to get the information under the stress and time pressure of an actual incident.

Looking ahead, it may be wise to build systems explicitly designed to obtain data to make this determination, and which can archive the decision-making process and rationale. As we have seen in the kinetic dimension,[10] we can almost be certain that cyber operations will be subject to exhaustive after-the-fact examinations aimed at accountability if things go awry—as will certainly be the case at some point.

On a related matter, if we are ever going to normalize cyberwar in the warfighting commander's toolkit, we are going to need robust systems that model the effects of a particular cyber technique.[11] We need this capability for two reasons; one is to help determine whether a cyber activity conducted by us, or against us, fulfills the Schmitt test so as to constitute the equivalent of a kinetic attack. As discussed, very different legal regimes flow from that critical, threshold determination.

If it equates to a kinetic strike against us, we then know we are likely free to conduct a national security response—whether that be diplomatic, economic, or military—as opposed to a law enforcement reaction. Similarly, if we are contemplating a cyber action that equates to a kinetic strike, a modeling capability will provide essential data to a decision-maker who must understand the effects in order to conduct a proportionality analysis, traditionally required under the law of war.[12]

---

10. Consider, for example, the attack on the Al Firdos bunker in 1991, when American aircraft dropped two 2,000 lb bombs on a hardened shelter. Despite clear indications of Iraqi leadership utilizing the bunker, many Iraqi civilians died or were injured in the attack. As a result, the basis for the American attack on the facility was closely and carefully scrutinized at the highest levels of government. *See generally* William Arkin, *The Battle for Hearts and Minds*, WASH. POST, 1998, http://www.washingtonpost.com/wp-srv/inatl/longterm/fogofwar/vignettes/v8.htm.

11. Such computer models would simulate how a particular type of attack would impact specific parts of cyber and physical infrastructure, as well as second- and third-order effects of such an attack.

12. The proportionality test is critical to assessing the legality of armed attacks. It embodies a balancing test whereby parties engaged in a conflict must evaluate whether civilian harm from an attack outweighs anticipated military advantages. *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 51(5)(b), June 8, 1977, 16 I.L.M. 1391, 1125 U.N.T.S. 17512 [hereinafter Protocol I] (prohibiting those attacks "which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated"). The principle is stated again in Article 57(2)(a)(iii), which requires military planners to "refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated." *Id.* at art.

Of course, the analysis does not stop at the "type of attack" determination, but next moves to a level of complexity embroiled with legal, policy, and even diplomatic entanglements. The real sticking point these days is a policy one, that is, the level of authority required to respond to an attack or launch a preemptory attack in light of a hostile threat or imminent attack.

As many of you know, that authority often rests at such a high level as to render a timely, viable response option almost impossible to implement. The bureaucratic coordination process renders potential cyber options too cumbersome for rapid, surgical responses. In my view, appropriate commanders must be given authority to utilize non-kinetic, or cyber, responses under the same rules that govern their use of weapon systems that result in kinetic effects. This "kinetic effects equivalency" is the "KEE" to making cyber responses a truly feasible option for commanders.[13]

The thorny questions, of course, often revolve around the legal parameters for cyber activities conducted under circumstances that invariably fall short of those that would justify the application of law of war principles.

Let me issue a clear warning. In the post 9/11 world, many legal experts believed that the President's commander-in-chief authority was readily applicable to threats presented by nontraditional actors such as terrorists and other subnational entities, and not subject to much in the way of other legal restraints.

In important ways, however, that concept of Presidential authority has been restricted by the courts. The Supreme Court's decision in *Boumediene v. Bush*,[14] released last June, is just the latest example. This is not to say that unilateral Presidential authority in the national security realm has been wholly eviscerated. Rather, it simply clarifies that the scope of that authority is more limited than some supposed.

I am particularly concerned about domestic cyber activity by the armed forces. I am not privy to what may or may not have been the involvement of military entities in domestic surveillance activities, but I would warn you that anything beyond activities very explicitly authorized by law must be avoided. You cannot be too careful here.

Apart from everything else, I believe that civilian agencies have much more robust capability[15] than may have existed in the after-

57(2)(a)(iii). This concept is considered to reflect customary international law, and therefore binding on states regardless of treaty obligations.

13. *See supra* notes 7–8 and accompanying text.

14. 128 S. Ct. 2229 (2008) (holding that a foreign national has a right to habeas corpus relief under the United States Constitution, and that the Detainee Treatment Act of 2005 is not an adequate and effective substitute for habeas corpus).

15. Using a Joint Interagency Task Force for Cyber could help harmonize federal action. *See* 6 U.S.C. § 465 (2002). DoD was recently tasked to develop and sub-

math of 9/11, so whatever exigency that may have existed is much diminished. Civilian agencies can and should take the lead today. Perhaps as, or more, important is consideration of the appropriate role of the armed forces in our democratic society.

Our nation has made the social and political decision to rely upon an all-volunteer force for the military element of national security. Historically, as the Supreme Court put it, the role of the armed forces is to "fight or be ready to fight wars should the occasion arise."[16] Today, however, the understanding of "war" is more complex, but I think the traditional notion of war is the lens through which the American people view their armed forces.

The vitality of the all-volunteer force depends upon the affection and respect of the American people for uniformed services. In fact, a June 2008 poll still shows the military as the institution in which the American people have the most confidence.[17] We cannot underestimate the importance of the linkage between the perception of the armed forces as an institution of integrity, and the disposition of America's mothers and fathers to encourage their sons and daughters to serve, not to mention the inclination of the best and brightest of our young people to spend the flower of their youth in uniform.

Nevertheless, America's positive image of our military is fragile and, actually, not really part of our heritage. Our founding fathers would be horrified at the size of today's standing military. It was not the structure they wanted.[18] In fact, throughout our history the American people have been, at best, ambivalent towards the professional military. It is only with the onset of the Cold War with the overarching Soviet nuclear threat that a sizable "peacetime" military was tolerated.

What I am trying to say is that any kind of domestic activity creates great risk to the reputation of the armed forces—a reputation it needs to sustain the domestic support it must have to maintain itself

---

mit to Congress a plan to improve and reform the Department's participation in, and contribution to, the interagency coordination process on national security issues. *See* Pub. L. No. 110-181 § 952, 122 Stat. 3 (2008).

16. United States *ex rel.* Toth v. Quarles, 350 U.S. 11, 17 (1955).

17. Jeffrey M. Jones, *Confidence in Congress: Lowest Ever for Any U.S. Institution* (2008), http://www.gallup.com/poll/108142/Confidence-Congress-Lowest-Ever-Any-US-Institution.aspx.

18. *See, e.g.* Letter from Thomas Jefferson to David Humphreys (1789), http://etext.virginia.edu/jefferson/quotations/jeff1480.htm (last visited Jan. 15, 2009) ("There are instruments so dangerous to the rights of the nation and which place them so totally at the mercy of their governors that those governors, whether legislative or executive, should be restrained from keeping such instruments on foot but in well-defined cases. Such an instrument is a standing army."); *see also,* Allan R. Milett, *The Constitution and the Citizen Soldier, in* THE UNITED STATES MILITARY UNDER THE CONSTITUTION OF THE UNITED STATES 1789–1989, 97–104 (Richard H. Kohn, ed. 1991).

as the world's premier military. There are almost no models in recent history where armed forces have been used for internal security purposes over extended periods that have been healthy for a democracy or, for that matter, good for the warfighting ability of military.

Importantly, there is perhaps no other society on earth that is more conscious of individual rights—to include privacy rights—than this country. And Americans guard their rights jealously, as should be the case. Thus, if people get the idea that the military is poking around in their private matters, reading their e-mails, and listening to their phone calls, the potential for resentment is huge.

If you doubt me on this, consider how Americans are insisting upon a panopoly of rights for the detainees of Guantanamo.[19] This is not sympathy for the terrorists themselves, but instead a concern for what our citizens perceive as affronts to rights they understandably believe define the American way of life.[20] Consequently, imagine if you will, their reaction if they perceive the military as part of a process that is anything other than scrupulously adherent to American law and values.

I do not at all dismiss the risk our adversaries pose to innocent Americans. Yet, we must recognize that our society readily pays an enormous price for personal freedom.

Consider that far more Americans have been killed in traffic accidents than by terrorists or insurgents since 9/11.[21] Consider also that in 2005, over 30,000 people in this country were killed by guns.[22] Yet, to date, this country has not imposed draconian restrictions on driving or gun rights. In short, we must *not* assume that Americans are willing to sacrifice their privacy and personal rights on the altar of security.

---

19. Criticisms of the United States' treatment of Guantanamo detainees abound among many civil rights groups. *See generally* Human Rights Watch, http://hrw.org/doc/?t=usa_antiterror (last visited Jan. 15, 2009) (containing multiple commentaries critical of Guantanamo detainees' treatment); Amnesty International, http://www.amnesty.org/en/counter-terror-with-justice (last visited Jan. 15, 2009) (containing similar commentaries); American Civil Liberties Union, http://www.aclu.org/safefree/detention/index.html (last visited Jan. 15, 2009).

20. *See* Boumediene v. Bush, 128 S. Ct. 2229 (2008).

21. For OIF/OEF fatality totals see OPERATIONS ENDURING FREEDOM & IRAQI FREEDOM CASULATY SUMMARY BY STATE (2009), http://siadapp.dmdc.osd.mil/personnel/CASUALTY/STATE_OEF_OIF.pdf. For statistics on US traffic fatalities from 1994 through 2006 see Fatality Analysis Reporting System, http://www-fars.nhtsa.dot.gov/Main/index.aspx. The latest traffic fatality rates in the United States can be viewed at Nat'l Highway Traffic Safety Admin., *Traffic Safety Facts* (2008), http://www-nrd.nhtsa.dot.gov/Pubs/811017.pdf.

22. Hsiang-Ching Kung et al., *Deaths: Final Data for 2005*, NAT'L VITAL STAT. REP., Apr. 24, 2008, at 10, *available at* http://www.cdc.gov/nchs/data/nvsr/nvsr56/nvsr56_10.pdf.

What I am suggesting is that it behooves the military in a free society to remain externally focused,[23] and I say that well aware of the borderless nature of cyberspace. That is why I believe that while we are developing a wide variety of technical tools and capabilities, their reach—to include their second and third order effects—must be fully understood before their employment.

For example, as recently as June the *Washington Post* had a cover story detailing the resurgence of Al Qaeda's web-based activities.[24] Under the law of war, there is nothing inherently wrong with destroying or distorting an adversaries' communication system.

Parenthetically, I am not among those who throw up their hands in despair at the challenge of impacting thousands of sites. Airmen have a long history of servicing thousands of targets over the course of an air campaign, so in my view, as an airman, doing so in the cyber realm is not quite as daunting as others may think.

Conceptually, however, it is one thing to attack an adversary's command and control capability, or to exploit their websites for intelligence purposes where there are ongoing combat operations, but quite another to attack their ideological message. The central legal and strategic issue is how do you focus your cyber activity specifically on the target? If you cannot do that, what is the effect on innocents?

For example, if we manipulate the website of an adversary so as to drive him to unproductive behaviors, or distort his message so as to unnerve his followers, what is our responsibility if that distortion is rebroadcast in some way back to the American people, as easily could be the case?

Suppose, for example, we manipulated cyber images to make it appear that an enemy leader was ordering an attack on a U.S. facility, and did so in order to flush his followers assembling for the attack onto a specific location of our choosing so we could destroy them. There is a clear military interest in doing so, but it may also have political implications on the American electorate. Specifically, such manipulated images of the enemy leader may have the effect of stiffening domestic political resolve that may be flagging in a given conflict. Determining the "rules of engagement," so to speak, for such activities is one of the main challenges for cyber-warriors.

---

23. *See* Richard H. Kohn, *Posse Comitatus: Using the Military at Home: Yesterday, Today, and Tomorrow*, 4 CHI. J. INT'L L. 165, 182–83 (2003) ("[R]egular armed forces need to face outward, against American enemies, rather than inward where a military force can become an institution acting on behalf of one part of the community against another. That corrodes the morale of the forces, harms recruiting, reduces readiness, undermines the support of the country for the armed forces, and ultimately drives a wedge between the military and society.").

24. Craig Whitlock, *Al-Qaeda's Growing Online Offensive*, WASH. POST, June 24, 2008, at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/06/23/AR2008062302135_pf.html.

Along these lines, I personally am increasingly convinced that the belligerent—today and in the future—with the most robust capability to determine the authenticity of information in our digitized world is the belligerent with a significant asymmetric advantage in cyberwar.

As you can tell, I am very wary of cyber modalities that cannot be limited to those who are "adversaries," within the meaning of traditional law of war. Where you are operating in environments not clearly within that realm, you are likely in what might be called a "law enforcement" legal regime. That regime does suffer legal impediments.

While I do not favor attempting to alter the law of war in some way to facilitate cyberwar, (an effort, I would argue, that would result in even *more* restraints) we do nevertheless need improved international cooperation to create legal architecture to better address the level of cyber activities not falling into the category where established law of war processes readily apply.

I know that any mention of the "law enforcement" regime causes cyber-warriors to grimace. As complicated and time consuming it may be, I think at this moment in history it is prudent for the U.S. to take a measured, collaborative approach with partner nations whenever possible. Otherwise, we risk having nations around the world individually, or collectively, raising new legal barriers.

While I recognize that nation-states may well be engaging in low-level activities and probes in order to prepare for what may be a major attack at some point, we should not necessarily conceive of the role of the military to address every attempted intrusion. It may well be prudent, for many reasons, to support civilian law enforcement agencies as the first line of defense for such probes, even for cyber actions aimed at domestic military facilities.

Quite candidly, I disagree with the "WarGames"[25] notion of the teenage hacker able to cause catastrophic damage from the computer in his bedroom. Some years ago, there may have been a "window of opportunity" where such scenarios might have occurred, but much has happened in the interim.

Yes, a terrorist might be able to manipulate this or that computer to deadly effect. However, only a nation-state, in my judgment, could cause the kind of debilitating damage that would equate to defeat in war. Accordingly, focus on that high-end threat does engender a set of legal issues under the law of war, but they are issues that play themselves out on mainly familiar legal ground.

I do have an observation for cyber-warriors. We will never be able to operationalize cyberspace to the same extent as has been done with the air weapon, absent a renewed effort to reduce the classification

25. WARGAMES (Metro-Goldwyn-Mayer 1983).

levels. Having been read into some cyber programs, it is remarkable how unremarkable they are relative to kinetic operations that are designed to achieve the same effects, but do not have the requirement for stratospheric clearances.

I sometimes think that classification levels are as much about rice bowls[26] and program control as they are about actual security needs. Regardless, the point is that reform and, perhaps, some risk assumption is necessary to fully socialize the idea of cyberspace operations.

Finally, as I indicated previously, while I am not keen on seeking to revise the law of war, per se, it may be the right time to consider strengthening the international legal norms related to cyber activities, especially those applicable in peacetime.

That said, I recognize those who believe that we should instead seek maximum flexibility, and be wary of any agreements that may result in tying our own hands. My personal view is that sometimes creating international norms for *peacetime* activities, especially through treaty law, gains favor in bipolar or multipolar worlds.

With respect to that, what is in the realm of the realistic? The seeds of collaboration are already scattered, for example in the Convention on Cybercrime ratified by the United States in 2006,[27] and in fragmentary restrictions scattered through other bodies of international law.

Whether consolidated in a unitary convention or strengthened in existing regimes, the scope of protections available is limited only by the imagination and the need for agreement. Possibilities offered by a number of people include:

- Reaffirming the sanctity of communications relay systems, including those in space—a regime begun under the Hague Convention of 1907 and elaborated upon under the International Telecommunications Union ("ITU");[28]

- Strengthening protections for communications systems and stations—elements of which can be found within the ITU and the Law of the Sea Convention;[29]

---

26. In military culture, the term "rice bowl" refers to a "jealously protected program, project, department, or budget; a fiefdom." Double Tongued Dictionary, http://www.doubletongued.org/index.php/dictionary/rice_bowl/ (last visited Jan. 15, 2009).

27. Council of Europe, Convention on Cybercrime, Nov. 23, 2001, C.E.T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [hereinafter *Cybercrime*].

28. Int'l Telecomms. Union, *Cybersecurity for All: ITU's Work for a Safer World* (2007), *available at* http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-CYBER-2007-PDF-E.pdf.

29. *See* United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1883 U.N.T.S. 397.

- Reinforcing the sanctity of navigational tools such as Tactical Air Navigation ("TACAN")[30] and the Global Positioning System ("GPS"),[31] including systems both terrestrial and those in space—a regime supported by the Chicago Convention[32] and International Civil Aviation Organization;

- Reaffirming the sanctity of arms control verification tools, especially those in space—a regime established through multiple arms control agreements;[33]

- Protecting supervisory control and data acquisition ("SCADA") systems that control critical infrastructure like dams, pipelines, and nuclear reactors;[34]

- Providing prohibitions and consequences for economic espionage;[35]

- Agreements to cooperate in cyber criminal investigations modeled on mutual legal assistance treaties ("MLATs") or the Cybercrime convention;[36]

- Creation of a tracking and logging regime to strip the anonymity of global hackers, much the way tracking materials can be embedded in high explosives to identify their origin;[37]

- Baseline speech restrictions—for example rules against terrorist incitement, bomb building instructions, exchange of computer network attack programs, and so forth—so long as such rules comply with domestic laws, such as the U.S. First Amendment;[38]

---

30. *See generally* Tactical Air Navigation, http://en.wikipedia.org/wiki/TACAN (last visited Jan. 15, 2009).
31. *See generally* Global Positioning System: Serving the World, http://www.gps.gov/ (last visited Jan. 15, 2009).
32. Convention on International Civil Aviation, Dec. 7, 1944, http://www.icao.int/icaonet/dcs/7300.html.
33. Treaty on the Principles Governing the Activity of States in the Exploration and Use of Outer Space Including the Moon and Other Celestial Bodies, Jan. 27, 2967, 18 U.S.T. 2410, 610 U.N.T.S. 207–208.
34. Brian T. O'Donnell & James C. Kraska, *Humanitarian Law: Developing International Rules of the Digital Battlefield*, 8 J. CONFLICT & SECURITY L. 133, 157–58 (2003) (discussing importance of developing technology systems to protect nation's infrastructure).
35. Susan W. Brenner & Anthony C. Crescenzi, *State-Sponsored Crime: The Futility of the Economic Espionage Act* 28 HOUS. J. INT'L L. 389, 447–51 (2006) (noting that as economic espionage enters cyberspace it becomes even more resistant to traditional law enforcement methods).
36. *Cybercrime*, *supra* note 27.
37. 27 C.F.R. 555.109 (2005), *available at* http://edocket.access.gpo.gov/2005/05-10618.htm (requiring manufacturers to place identifying marks on explosive materials for sale or distribution).
38. U.S. CONST. amend. I.

Serious consideration could be given to each provision to determine whether derogation should be permitted during international armed conflict, and if so, what notification or protection regimes might be required to avoid collateral civilian consequences.

For those provisions that are derogable,[39] the DoD could continue to groom trained and equipped cyber-warriors ready to unleash kinetic and cyber effects upon the enemy. Certainly, there is evidence other nations are undertaking similar efforts.[40]

Cyberspace has evolved beyond the imagination of most in the last fifteen years to the point that science fiction has become more science than fiction.[41] But it stands on a precarious foundation that could be shaken by a cyber 9/11 or cyber Pearl Harbor. Who has forgotten that after 9/11 the skies were emptied of aviation? Who has suffered

39. A non-derogable provision of a treaty may not be violated or suspended under any circumstance. In contrast, under some human rights treaties, a state can formally file a notice of derogation for derogable rights during a state of emergency. *See e.g.*, International Covenant on Civil and Political Rights art. 4(1), Mar. 23, 1976, 6 I.L.M. 368, 999 U.N.T.S. 171.

40. See, e.g., 2008 NATIONAL DEFENSE STRATEGY, *supra* note 5, at 22 (declaring specifically that "China is developing technologies to disrupt our traditional advantages. Examples include development of anti-satellite capabilities and cyber warfare."). Such a perspective is not new. *See* John A. Serabian, Jr., Info. Operations Issue Manager, CIA, Statement for the Record Before the Joint Economic Committee on Cyber Threats and the U.S. Economy (Feb. 23, 2000), https://www.cia.gov/news-information/speeches-testimony/2000/cyberthreats_022300.html ("We are detecting, with increasing frequency, the appearance of doctrine and dedicated offensive cyber warfare programs in other countries. We have identified several, based on all-source intelligence information, that are pursuing government-sponsored offensive cyber programs. Foreign nations have begun to include information warfare in their military doctrine, as well as their war college curricula, with respect to both defensive and offensive applications. They are developing strategies and tools to conduct information attacks. Those nations developing cyber programs recognize the value of attacking adversary computer systems, both on the military and domestic front. Just as foreign governments and the military services have long emphasized the need to disrupt the flow of information in combat situations, they now stress the power of cyber warfare when targeted against civilian infrastructures, particularly those that could support military strategy.").

41. For example, cyber techniques were apparently used before and during the 2008 conflict in Georgia. *See* David Ho, *Web Sites Hit As War Uses Bytes and Bullets*, ATLANTA J.-CONST., Aug. 15, 2008, at 1, *available at* http://www.ajc.com/metro/content/printedition/2008/08/15/cyberwar.html ("As Russian tanks roll through Georgia, the assault is continuing in another realm: cyberspace, where hackers are waging war on Georgian Web sites, e-mail and communication services. About 20 Georgian government, banking and media sites were offline Thursday, said Scott Borg, director of the U.S. Cyber Consequences Unit, an independent research group that advises the government. Some sites have fled to hosting computers elsewhere . . . but are continuing to take digital fire. The ongoing online battle, which appears to have begun before the first shots were fired, is a preview of a new era in warfare—one for which the United States is not ready, government officials and security experts say.").

through an extended blackout or loss of water? Who has contemplated the impact of a fuel shock on the global economy, especially as gas passes $4.00 per gallon? Cyberspace is as vital as those resources and intimately connected to them as well.

For that reason I say again, welcome cyber-warriors; especially cyber-defenders. Our nation's future depends on you.