Changing the Paradigm of Internet Access from Government Information Systems: A Solution to the Need for the DOD to Take Time-Sensitive Action on the Niprnet

Joshua E. Kastenberg
University of New Mexico

Follow this and additional works at: http://digitalrepository.unm.edu/law_facultyscholarship

Recommended Citation
Available at: http://digitalrepository.unm.edu/law_facultyscholarship/435
CHANGING THE PARADIGM OF INTERNET ACCESS FROM GOVERNMENT INFORMATION SYSTEMS: A SOLUTION TO THE NEED FOR THE DOD TO TAKE TIME-SENSITIVE ACTION ON THE NIPRNET

LIEUTENANT COLONEL JOSHUA E. KASTENBERG

I. INTRODUCTION .......................................................................... 176
II. THE NATURE OF DOD CYBERSPACE: CURRENT ASSUMPTIONS AND DANGERS ................................................... 178
III. INADEQUACIES OF CURRENT REGULATIONS ........................................... 183
   A. Joint Ethics Regulation .................................................................. 184
   B. Other DOD-Wide Regulations ......................................................... 188
   C. Service Rules and Regulations ....................................................... 189
IV. COURSES OF ACTION ................................................................... 192
   A. Lawful Order ............................................................................. 192
   B. Regulations ............................................................................... 195
   C. Hybrid Approach ........................................................................ 197
   D. Support from Other Jurisdictions ................................................ 198
V. CONCLUSION ............................................................................. 200

APPENDIX. PROPOSED DOD DIRECTIVE AND DRAFT ORDER ............202

Lieutenant Colonel Joshua E. Kastenberg (B.A., University of California, Los Angeles (1990); J.D., Marquette University (1996); LL.M., Georgetown University (2003)) is the Staff Judge Advocate, 332d Air Expeditionary Wing, Balad Air Base, Iraq. Prior to his current assignment, he served as the Staff Judge Advocate, Joint Task Force-Global Network Operations, a standing joint task force under the command of United States Strategic Command. Under the Unified Command Plan, it is the sole cyber-defense operational command for the Department of Defense. He is a member of the Wisconsin Bar.
I. INTRODUCTION

On 12 May 2008, the Deputy Secretary of Defense (Dep SECDEF) issued a formal definition of cyberspace via a memorandum to the secretaries of the military departments and the rest of the Department of Defense (DOD). Implicit in this memorandum was a statement of the importance of cyberspace to military operations. Specifically, the Dep SECDEF noted that combatant commands and other defense components require "the ability to operate unhindered in cyberspace." Thus, it is now doctrinally accepted, without any exception within the DOD, that cyberspace is a "war-fighting domain."

However, cyberspace is a domain not only used by war-fighters (indeed warfighters are a miniscule minority of users), it is accessed by a significant and growing global population for business

---

1 Memorandum from Deputy Secretary of Defense to Secretaries of the Military Departments et al., subject: The Definition of “Cyberspace” (12 May 2008) [hereinafter Dep SECDEF Memo]. The memorandum defines cyberspace as: “A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.” Id.; see also U.S. DEP’T OF DEF. JOINT PUB. 1-02, DICTIONARY OF MILITARY AND ASSOCIATED TERMS, 141 (12 Apr. 2001, as amended through 17 Mar. 2009). This definition is bolstered in part by U.S. DEP’T OF DEF. DIR. 8320.02, DATA SHARING IN A NET CENTRIC DEPARTMENT OF DEFENSE para. 4.1 (23 Apr. 2007) [hereinafter DODD 8320.02], which states, “Data is an essential enabler of network-centric warfare (NCW) and shall be made visible, accessible, and understandable to any potential user in the Department of Defense as early as possible in the life cycle to support mission objectives.”

2 Dep SECDEF Memo, supra note 1.

3 See, e.g., Lieutenant General Keith Alexander, Warfighting in Cyberspace, 46 JOINT FORCE Q. 58, 58-61 (3d Quarter 2007); General James E. Cartwright, USSTRATCOM, a Command for the 21st Century, 42 JOINT FORCE Q. 71 (3d Quarter 2006); JOINT CHIEFS OF STAFF, JOINT PUB. 3-11, JOINT OPERATIONS, at III-22 (13 Feb. 2008) [hereinafter JP 3-11]; JOINT CHIEFS OF STAFF, JOINT PUB. 3-13 INFORMATION OPERATIONS, at I-4 (13 Feb. 2006) [hereinafter JP 3-13]. A facet of cyberspace as a warfighting domain was already accepted in terms of net-centric warfare (NCW). See, e.g., DODD 8320.02, supra note 1, at E 1.1.18 which defines NCW as:

An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.

Also note, in the 2004 National Military Strategy for the United States, the Chairman of the Joint Chiefs of Staff noted “the Armed Forces must have the ability to operate across the air, land, sea, space and cyberspace domains of the battlespace.” CHAIRMAN OF THE JOINT CHIEFS OF STAFF, NATIONAL MILITARY STRATEGY OF THE UNITED STATES 18 (unclassified version, 2004) [hereinafter NAT’L MIL. STRATEGY].
communications, personal recreation, intelligence collection, and a host of other uses. Commensurately, cyberspace is a crowded domain, and for the warfighter, access to it requires cleared pipelines, in turn necessitating a minimization of unofficial Internet access. The DOD does not own cyberspace, or even a portion of it, in a traditional legal sense. But, the DOD is able to perform functions in parts of cyberspace by creating security measures which control access to those areas. The area of operations controlled by the DOD is referred to as the Global Information Grid (GIG). Without access to the GIG, or the ability to protect the flow of information (or freedom of maneuver) on it, the military's capabilities are severely degraded.

It is axiomatic that the success or failure of military operations in cyberspace is contingent on access to cyberspace. While much of the focus on the military's use of cyberspace is on offensive or defensive roles, attention to the management of access to cyberspace is equally important. This is because without proper management, neither the full

---

4 U.S. DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY TO SECURE CYBERSPACE, (February 2003) [hereinafter NATIONAL CYBERSPACE STRATEGY]. This article's argument comports with the third of five priorities set out in the Strategy, to raise national cybersecurity awareness.


7 U.S. DEP'T OF DEF., DIR 8100.01, GLOBAL INFORMATION GRID, OVERARCHING POLICY para. E.2.1.1 (Sept. 19, 2002; certified current Nov. 21, 2003) [hereinafter DODD 8100.00], defines cyberspace as, the notional environment in which digitized information is communicated over computer networks. The DOD portion of cyberspace is referred to as the Global Information Grid, or "GIG." DODD 8100.01 defines the GIG as:

The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services necessary to achieve Information Superiority.

range of offensive, defensive, or exploitive operations will occur. However, the DOD is currently lacking sufficient regulatory authority to ensure the availability of access to conduct operations through cyberspace, because the conduct of its members is predicated on a number of false assumptions which are written into outdated or otherwise poorly designed current regulations. This article addresses those assumptions and existing regulations and argues for new guidance to alter the current paradigm of almost unfettered access.

This article is divided into three sections. Section I touches on the nature of DOD cyberspace and the potential harms that result from current social behaviors of the department’s personnel. Section II analyzes shortcomings in existing regulations to police the use of government information systems. Section III presents differing options to provide the DOD and its commanders a means to reduce the risk of malicious code through the implementation of a new regulation or lawful order. It also includes an analysis of relevant supportive federal and state court decisions. Finally, the article contains an appendix with a draft proposed regulation and a draft order. One issue throughout this article is important to note. The article and its contents are unclassified, but much of the information on cyber-intrusions, defense methods in the networks, and the forensic work on malicious codes are classified secret and top-secret. Consequently, the article relies on open source documents, which do not contain detailed information on the tactics, techniques, and procedures or adversary conduct in cyberspace.

II. THE NATURE OF DOD CYBERSPACE: CURRENT ASSUMPTIONS AND DANGERS

There are five essential considerations which require continual understanding throughout this article, and indeed, in addressing the need to change the paradigm of almost unfettered access. The first is social behavior, which is the sole focus of this article. Most users believe that access to the internet is of only nominal cost, which results in its

---

9 Offensive actions fall under the rubric of Computer Network Attack (CNA) which is doctrinally defined as “actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.” JP 3-13, supra note 3, at II-5. Defensive actions fall under the rubric of computer network defense (CND) which is doctrinally defined as “actions taken . . . to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks.” Id. Intelligence and other activities on the network, such as operations preparation of the battlespace, generally fall under the rubric of computer network exploitation (CNE). Id. CNE is defined as enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Id.
unfettered use. This assumption is false. In fiscal year 2007, the DOD through the Defense Information Services Agency procured Internet access at an annual recurring cost in excess of $105 million. In July 2008, a naïve e-mail user in the DOD sent out an e-mail containing an Internet game attachment. The resulting e-mails and other net activity caused a widespread disruption across the base’s server.

Despite the expenditure of monies, freedom of access to the internet has also translated into the idea that the DOD or its component services will block offending or dangerous sites. Problematic to this assumption is that many otherwise legitimate sites unwittingly contain malicious code, and other sites are spoofed to enable exfiltration of critical data. The National Institute of Standards and Technologies (NIST), a division of the Department of Commerce, states the problem as this: “In the 1980s, malware was occasionally a nuisance or inconvenience to individuals and organizations; today, malware is the most significant external threat to most systems, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations.”


14 NAT’L INST. OF STANDARDS & TECH., SPECIAL PUB. 800-83, GUIDE TO MALWARE INCIDENT PREVENTION AND HANDLING 2-1 (NOV. 2005) [hereinafter NIST SP 800-83]. NIST recommendations are not binding on government agencies, and in particular, national security systems are exempt from NIST directives.

Organizations should plan and implement an approach to malware incident prevention based on the attack vectors that are most likely to be used, both currently and in the near future. Because the effectiveness of prevention techniques may vary depending on the environment (i.e., a technique that works well in a managed environment might be ineffective in a non-managed environment), organizations should choose preventive methods that are well-suited to their environment and systems. An organization’s approach to malware incident prevention should incorporate policy considerations, awareness programs for users and information technology (IT) staff, and vulnerability and threat mitigation efforts.
Moreover, while it is true technologies exist to block access to specific websites, it is also true that technologies exist to bypass those web-blocks, and as such, have already been employed by service-members and other DOD personnel. While accessing Internet sites from DOD computers posses only one risk to malicious code, it is the most difficult to prohibit. For instance, it is likely easier to prevent the transfer of information from a personal computer via a personal thumb-drive or other removable media to a DOD computer than it is to prohibit access to sites which are not currently blocked. In response to the appearance of malicious code on government information systems of various classification levels, the DOD enacted a ban on the use of certain removable media. At best, technological solutions alone deprive the DOD of the full “defense in depth” that it requires to protect its cyber capabilities or critical information.

The second consideration is that risks such as malicious code occur as a function of access and connection, rather than actual time spent on an Internet site. The time to download a malicious code is often measured in nanoseconds, making it virtually instantaneous. Malicious code resides primarily across the Internet, but some malicious code has been designed to traverse onto computer systems with high classification levels that do not connect to the Internet. Gaps, known colloquially as “air gaps,” existing between isolated classified system networks and unclassified systems connecting to the Internet were thought to serve as a protective barrier against intrusions onto the

---

15 A good discussion of this problem in found in Nat’l Inst. of Standards & Tech., Special Pub. 800-28-v2, Guidelines on Active Content and Mobile Code 3-3 (Mar. 2005) [hereinafter NIST SP 800-28-v2].
16 Nat’l Inst. of Standards & Tech., Special Pub. 800-53-r2, Recommended Security Controls for Government Information Systems B-6 (Dec. 2007) defines malicious code as software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system, such as a virus, worm, Trojan Horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
19 See, e.g., Neal Kumar Katyal, Criminal Law in Cyberspace, 149 U. Pa. L. Rev. 1003, 1023-26 (2001). A good discussion on the subject of malicious code is also found in State v. Corcoran, 522 N.W.2d 226 (Wis. Ct. App. 1994).
classified systems.\textsuperscript{21} But, information on the classified systems as well as the systems themselves may be in jeopardy by both the lawful transference of information, as well as the negligent transference of information between the classified levels.\textsuperscript{22} As a result, this article is not concerned with the ethical implications of time spent in web-surfing from government information systems during duty hours, but the web-surfing itself.

The third consideration is what the reduction in unofficial Internet access traffic will give commanders overseeing military operations. United States military operations rely on decisional superiority, freedom of maneuver, and operational security.\textsuperscript{23} Because of excessive unofficial Internet usage, the DOD decided to purchase commercial Internet service in the U.S. Central Command area of responsibility. The reduction in unofficial Internet access traffic will protect these essential operational requirements by reducing the risk to the GIG.

Fourth, the exponential growth of malicious code risks to secured information on the GIG, the ability for the DOD to freely access the GIG, and the integrity of secured information on the GIG are all part of the same concern: GIG security. While no regulation, however austere, will remove all risks, it is very apparent that nation-states and non-state actors have engaged in robust exfiltration of data from government information systems, including the DOD's systems.\textsuperscript{24}

\begin{footnotes}

\begin{quote}
The only foolproof protection against penetration of a system is an "air gap." The only way that a computer or a networked office can be fully protected from hackers is to have a physical gap separating every computer in that office system from the Internet or the telephone system. The term "air gap" means an absolute communications gap between the computer system and the Net or the telephone.
\end{quote}

However, wireless technology has rendered this type of security obsolete.

\textsuperscript{22} "Air gap" architecture is explained in BIDGOLI, \textit{INFORMATION SECURITY}, supra note 18, at 522-524.

\textsuperscript{23} These factors are found in a number of Executive Statements and DOD publications. See, e.g., NAT'L MIL. STRATEGY, supra note 3, at 15-19; U.S. DEP’T OF DEF. DIR. 5205.2, OPERATIONAL SECURITY (OPSEC) PROGRAM (29 Nov. 1999) [hereinafter DODD 5205.2].

\end{footnotes}
Moreover, the 2007 Estonian experience, in which denial of service attacks encumbered that allied government’s ability to rely on its information systems, must concern the integrity of DOD systems.\textsuperscript{25} Fifth and finally, a definition of official use and unofficial use in terms of Internet access does not currently exist in the DOD lexicon. For the purpose of this article, unofficial use is defined as a use which does not relate to the functions or necessities of DOD personnel or mission sets.\textsuperscript{26} For instance, individuals accessing weather information in preparation for a TDY or real estate information in preparation for a permanent change of station (PCS) move may articulate the search as related to official duty. On the other hand, when individuals access those same sites prior to a personal vacation or for non-PCS investment reasons, there is little likelihood the same articulation to mission nexus can occur.

Access to the Internet from any location occurs with a number of inherent risks. These risks include the transfer of malicious code, which may be designed to remotely corrupt or commandeer a computer system, destroy the system, implant a virtual beacon on the system to provide information to a far-way user, or convey false information through the user’s system.\textsuperscript{27} One recent study concluded that 80\% of legitimate sites have malicious code implanted.\textsuperscript{28} The exponential growth of malicious codes has affected the DOD systems, making them increasingly vulnerable to the risks noted above. Technical solutions provide only a short-term solution and a partial insurance against these


\textsuperscript{26} This definition is taken in part from U.S. DEP’T OF DEF. JOINT PUB. 1-02, DICTIONARY OF MILITARY AND ASSOCIATED TERMS, supra note 1, which defines “Official Information” as “information that is owned by, produced for or by, or is subject to the control of the United States Government.” Id. at 390.


risks, primarily because the ability of malicious code developers matches the ability of security advances.

Like most computer networks, DOD computer information systems provide a ready access to the Internet. During any given twenty-four hour period the Internet is accessed over one billion times from roughly seven million DOD owned computers. The overwhelming majority of this traffic occurs on the Non-Secure Internet Protocol Router Network (NIPRNET). In an ongoing study, over two-thirds of Internet access from DOD computers occurs for non-official purposes. The types of sites accessed including dating services, resort and vacation sites, car purchases, electronic stock and commercial trading, sports sites, and “streaming video” sites. While it is remotely possible a small minority of users accessing these sites could argue the access occurred for an official DOD purpose, one would be hard pressed to believe the bulk of the access was for a mission-related function.

Despite the fact that the NIPRNET is non-secure, a number of protected, encrypted, or coded DOD functions occur across it. These functions include pay and leave access, transfer and tracking of component parts, the bulk of aircraft schedules, medical information transfers, fuel data, travel schedules of ranking officers and civilian personnel, real-time communications, and a variety of other data which is closely guarded and essential for military operations. Moreover, information may be transferred to and from the NIPRNET to the Secured Internet Protocol Router Network (SIPRNET), as well as higher classified systems, placing the higher classification of SIPRNET and other access data at risk.

III. INADEQUACIES OF CURRENT REGULATIONS

Prior to examining current departmental and service regulations, it is essential to examine 10 U.S.C. § 2224, which directs SECDEF to develop and maintain a “Defense Information Assurance Program.” The regulations examined below, in some measure, are buttressed by this law. For instance, it requires this program to “provide continuously

---

30 DEF. INFO. SERVICES AGENCY REPORT (2007) (delivered to U.S. Congress, on file with author and DISA).  
31 JOINT TASK FORCE GLOBAL NETWORK OPERATIONS REPORT (2008) (delivered to the Joint Chiefs of Staff, on file with author).  
32 Id.  
33 Id. Higher systems include Intelligence Community (IC) networks.  
for the availability, integrity, authentication, confidentiality, nonrepudiation, and rapid restitution of information and information systems that are essential elements of the Defense Information Infrastructure." It additionally charges SECDEF to develop a program strategy that encompasses those actions necessary to assure the readiness, reliability, continuity, and integrity of Defense information systems, networks, and infrastructure.

But, as noted in the introduction, regulatory authorities do not adequately address network threats to the DOD's mission capabilities, and this fact shows a failing to comply with 10 U.S.C. § 2224. Moreover, the regulations containing rules governing Internet access are disjointed. These include departmental regulations, Chairman of the Joint Chiefs of Staff Instructions, service regulations, and individualized user agreements. Moreover, while rescission of security clearances based on Internet misuse has also been sustained by administrative law judges, this is merely a "backdoor" method for addressing the problem and available in only limited circumstances.

For reasons noted below, none of these regulations satisfactorily mitigates the threats described above.

A. Joint Ethics Regulation

Department of Defense Directive 5500.7-R, the Joint Ethics Regulation (hereafter JER) governs the conduct of all DOD personnel. It was most recently updated on November 29, 2007. The JER was promulgated to buttress public trust in the Department of Defense. It also serves as a mirror to the Code of Federal Regulations (CFR) and other government instruments serving the same purpose.

---

38 U.S. DEP'T OF DEF., DIR. 5500.7-R, JOINT ETHICS REG. (30 Aug. 1993) (C6, 29 Nov. 2007) [hereinafter JER]. The Department of Defense General Counsel manages the Joint Ethics Regulation and all programs underneath it. Id. § 1-407.
39 Id. at 43.
40 Id. § 1-300.
41 See Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. § 2635 (1978). Department personnel are also required to comply with 5 C.F.R. § 2635.101(a) which states:

Public service is a public trust. Each employee has a responsibility to the United States Government and its citizens to place loyalty to the Constitution, laws and ethical principles above
The JER governs such areas as political activities, relationships between DOD personnel and contractors, gifts between superiors and subordinates, expenditures of government monies for conferences, and attendance at private events. The JER’s primary strengths are that it is the most holistic governance for DOD personnel in regard to professional behavioral standards and it does not contradict the Uniform Code of Military Justice (UCMJ). Moreover, the JER provides the due process notice requirements for enumerated military offenses under which violations may be charged.\footnote{42} Violations of the JER may be charged against persons subject to the UCMJ through Article 92.\footnote{43}

At first glance, the JER should provide some authority to regulate unofficial access to the Internet because it is a fundamental principle of administrative law that an agency is bound to adhere to its own regulations.\footnote{44} However, as a disciplinary tool, the JER has rarely served as the basis for charging UCMJ offenses in courts-martial. Indeed, the appellate record of published cases is slim. In United States\textit{ v. Crafter},\footnote{45} the Court of Appeals for the Armed Forces (CAAF) upheld a court-martial conviction based on the provision of the JER prohibiting bribery.\footnote{46} CAAF has also upheld a conviction for accessing child pornography and bestiality websites charged under the JER.\footnote{47} However,

\footnote{42} See, e.g., Parker v. Levy, 417 U.S. 733, 755 (1974) (An accused must be on notice that his conduct is unlawful and that the article fairly informs "that the particular conduct which he engaged in was punishable"). Although the notice requirement of the Joint Ethics Regulation has apparently not been challenged at the appellate level, it is reasonable to assume it meets this due process standard.

\footnote{43} See MANUAL FOR COURTS-MARTIAL, UNITED STATES pt. IV, ¶16a (2008) [hereinafter MCM].

\footnote{44} Frizelle v. Slater, 111 F.3d 172, 177 (D.C. Cir. 1997).

\footnote{45} United States v. Marcum, 60 M.J. 209 (C.A.A.F. 2006).

\footnote{46} Id. at 210. The specification read:

[D]id, at or near Seymour Johnson Air Force Base, on or about 9 May 9 2002, violate a lawful general regulation, to wit: the Joint Ethics Regulation, Department of Defense Directive 5500.7-R, Chapter 5, ¶ 5-400(a), dated 30 August 1993, by wrongfully accepting currency of some value for arranging for Federal Prison Camp Inmate [G] to meet in private with his friend [Ms. ADP] at a billeting room at the Southern Pines Inn, a willful violation of [his] lawful duties to supervise the work of the said Federal Prison Camp Inmate.

bribery and child pornography are already prohibited in other regulations, raising the question as to why the JER was incorporated into a UCMJ charge and specification in the first place.

Civilian employment within the DOD has been terminated on the basis of JER violations as well, but only rarely. The Merit Systems Protection Board (MSPB), the primary governing body for adjudicating challenges to adverse employment decisions, has upheld agency decisions to terminate employment for such reasons as monetary debts to subordinates, using government computers for personal business and sending sexually suggestive e-mails to other employees, accepting gifts from subordinates exceeding the amount permitted under the regulation, and, sexual harassment.

However, it does not appear that under either the JER, or its incorporation under the UCMJ, that any charges have occurred for excessive unofficial non-pornographic Internet access or access for personal recreational purposes. Accessing pornography has been amply charged against both uniformed service members and non-uniformed DOD employees but usually not under the JER.

In terms enabling the sought-after paradigm change, the JER possesses inherent weaknesses beyond the obvious statistical evidence. To begin, the regulation in section 2-301 lumps computer use in the same category as other modes of government-owned communications, to include telephones and facsimile machines. While service members have been prosecuted for using government telephones, military law favors charging unofficial telephone use under UCMJ, Article 121, prohibiting larceny, rather than under the JER. It would be difficult to charge unofficial access to the Internet under the same article prohibiting larceny because that particular article requires the government to prove the user's intent to permanently deprive the owner of a property, that the property had a rightful owner, and that the property had an actual value, or at least some nominal value.

---

49 Barnes v. Dep't of Def., 2006 MSPB LEXIS 3148 (Merit Systems Protection Board 2006).
50 Siozon-Peterson v. Dep't of the Air Force, 2005 MSPB LEXIS 2067 (Merit Systems Protection Board 2005).
51 Reynolds v. Dep't of the Army, 2003 MSPB LEXIS 1087 (Merit Systems Protection Board 2003).
52 JER, supra note 38, § 2-301(a).
53 See, e.g., United States v. Cornell, 15 M.J. 932 (C.M.A. 1983) (determining that personal telephone use could be charged as larceny, instead of under the JER); United States v. Abeyta, 12 M.J. 507 (A.C.M.R. 1981) (determining that personal telephone use could be charged as larceny, instead of under the JER).
54 MCM, supra note 43, pt. IV, ¶ 46b(1); see also United States v. Batiste, 11 M.J. 791 (A.F.C.M.R. 1981) (theft of urine sample a proper charge for larceny even though urine generally possesses no known value). Unlike urine, which has a theoretical owner, it is
The JER does not take into account the risk to the GIG or the nature of the NIPRNET. Indeed, it does not even make use of those terms anywhere within its voluminous rules. Telephones and facsimile machines do not, as a general rule, have the capability of transferring malicious code, serve as an effective tool for the exfiltration of data, or possess the inherent capability of a takeover from an operator at a remote site.

Section 2-301(a) governs the use of DOD computers under the aegis of "Use of Government Resources." The regulation defines official use to include such matters as: emergency communications, communications to military members and other DOD employees who are deployed or in extended TDY status.

Yet, the regulation permits commanders flexibility to permit DOD personnel at a normal workplace to conduct brief internet searches beyond matters involving official business or family communications under certain conditions reflecting the overarching ethics rules. The JER does not define brief internet searches, leaving one to conclude that the content of such searches are only constrained by what is already prohibited under other regulations or laws such as pornography, child pornography, gambling, or political activities.

As a further example of the regulation's permissive nature, wide-ranging Internet searches are permitted when that activity does not adversely affect the performance of official duties of the DOD employee or organization. Although the regulation does not define the term unlikely the prosecution could claim that the government was deprived of the GIG or that the GIG possesses a quantifiable — albeit nominal — value. It may be the case that the Internet is public and therefore abandoned property. See, e.g., United States v. Meeks, 32 M.J. 1033, 1035-1036 (A.F.C.M.R. 1992); United States v. Walls, 2 C.M.R. 650 (A.F.B.R. 1951). Moreover, the proof required to determine that a user who accesses the Internet for unofficial uses intended to deprive the government of its property could not likely be met by any reasonable quantum.

55 See JER, supra note 38, § 2-301(a). The JER notes: "Federal Government communication systems and equipment (including Government owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems when in use is paid for by the Federal Government) shall be for official use and authorized purposes only."

56 Id.

57 JER, supra note 38, § 2-301(a)(2)(d) reads:

Do not put Federal Government communication systems to uses that would reflect adversely on the DOD or the DOD Component (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violations of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service) . . . .

Internet Access from Government Information Systems
"brief," it permits use that is of "reasonable duration and frequency" and serves "a legitimate public interest." The regulation does not define "legitimate public interest," but it provides examples such as "enhancing the professional skills of" DOD employees or "job searching." Therein is the proof that the JER's drafters missed the fundamental risk factors in Internet access in that it is a matter of access and not time spent on any particular activity which creates risk in the first place.

B. Other DOD-Wide Regulations

Other regulations exist which govern the use of the government information systems as well as the GIG, but none directly addresses the social behaviors of accessing the Internet. For instance, DODD 8500.01 E, 

Information Assurance,

articulates policy to regulate access to the internet, but primarily through technological solutions. Its implementation instruction, DODI 8500.2, 

Information Assurance (IA) Implementation,

places on all DOD personnel the responsibility to only access data for "which they are authorized or have a need to know." While 8500.02 provides defined language, it is not a regulation under which DOD personnel may be disciplined for unofficial Internet access, though arguably if the access resulted in damage or disruption to

DOD information systems shall regulate remote access and access to the Internet by employing positive technical controls such as proxy services and screened subnets, also called demilitarized zones (DMZ), or through systems that are isolated from all other DOD information systems through physical means. This includes remote access for steelwork.

DOD information systems shall regulate remote access and access to the Internet by employing positive technical controls such as proxy services and screened subnets, also called demilitarized zones (DMZ), or through systems that are isolated from all other DOD information systems through physical means. This includes remote access for steelwork.

---

58 See JER, supra note 38, § 2-301(a)(2)(b).
59 Id. § 2-301(a)(2)(c).
60 Id.
61 U.S. DEP'T OF DEF. DIR. 8500.01 E, INFORMATION ASSURANCE (Oct. 24, 2002; certified current as of Apr. 23, 2007) [hereinafter DODD 8500.01 E].
62 Id. para. 4.12.
63 U.S. DEP'T OF DEF. INSTR. 8500.2, INFORMATION ASSURANCE (IA) IMPLEMENTATION (Feb. 6, 2003) [hereinafter DODI 8500.2].
64 Id. para. 5.12.
DOD information systems, DOD personnel might become the subject of an investigation.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI), 6211.02C, Defense Information Systems Network (DISN) Policy, Responsibilities, and Processes, imposes responsibility on all DOD personnel to protect classified information, including classified information on DOD networks. It also provides parameters of "authorized uses" for government information systems capable of accessing the internet. But the parameters for acceptable Internet access in this instruction mirror those in the JER. CJCSI 6510.01E, Information Assurance (IA) and Computer Network Defense (CND), provides additional authority to hold accountable individuals who place government information systems at risk through negligent conduct or intent. The range of accountability includes terminating an individual's ability to access the Internet from a government information system. However, CJCSI 6510.01E does not require combatant commands, services, and agencies to reduce the amount of Internet access.

C. Service Rules and Regulations

Army Regulation (AR) 25-1, Knowledge Management and Information Technology, establishes the policies and assigns responsibilities for the management of information resources and

---

65 CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION 6211.02C, DEFENSE INFORMATION SYSTEM NETWORK (DISN): POLICY, RESPONSIBILITIES AND PROCESSES (9 Jul. 2008) [hereinafter CJCSI 6211.02C].
66 Id. encl. B, para. 9.r.

DOD and non-DOD personnel (including supporting contractor personnel) are held personally and individually responsible and accountable for providing proper protection of classified information, controlled unclassified information, ISs, and/or networks under their custody and control. DOD officials who hold command, management (e.g., DAA and Information Assurance Manager), or supervisory positions (e.g., Information Assurance Officer or supervisors) will ensure that the Information Security Program is efficiently implemented and managed within their areas of responsibility.

67 Id., para. n.
68 CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION 6510.01E, INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE (CND) (15 Aug. 2007, current as of 12 Aug. 2008) [hereinafter CJCSI 6510.01E].
69 While this document articulates roles and responsibilities of commands and individuals, a CJCSI is not a regulation of a punitive nature.
information technology. This regulation governs internet access for all personnel assigned to, or employed by, the Department of the Army. While the entirety of AR 25-1 is not punitive, the regulation notes there are punitive portions.

Of importance, unlike the JER, the authors of AR 25-1 evidenced their understanding of the GIG by incorporating and defining the NIPRNET and SIPRNET into the regulation. Notably, AR 25-1 prohibits computer activity "that could reasonably be expected to" congest, delay, or disrupt computer service.

In one sense, the language contained in AR 25-1 is superior to that found in the JER. Specific intent is not the liability standard for violations. Thus only a general negligence of Internet access which

---

71 Id. at i. The regulation notes, "Portions of this regulation, which prescribes specific prohibitions, are punitive, and violations of these provisions may subject offenders to nonjudicial or judicial action under the Uniform Code of Military Justice." Id.
72 Id. at para. 6-1.f(5) (prohibiting the use of Army communications systems in ways "that could reasonably be expected to cause, directly or indirectly, congestion, delay, or disruption of service to any computing facilities or cause unwarranted or unsolicited interference with others' use of communications") While the regulation provides examples of conduct which could cause a detriment, the list is not all-inclusive. The list reads:

(a) Create, download, store, copy, transmit, or broadcast chain letters.
(b) "Spam" to exploit list servers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited e-mail.
(c) Send a "letter-bomb" to re-send the same e-mail message repeatedly to one or more recipients, to interfere with the recipient's use of e-mail.
(d) Broadcast unsubstantiated virus warnings from sources other than systems administrators.
(e) Broadcast e-mail messages to large groups of e-mail users (entire organizations) instead of targeting the relevant audience.
(f) Employ applications for personal use using streaming data, audio, and video; malicious logic and virus development software, tools, and files; unlicensed software; games; Web altering tools/software; and other software that may cause harm to Government computers and telecommunications systems.
(g) Disseminating large files over e-mail instead of using shared drives.

Id.
73 See, e.g., United States v. Hernandez-Landaverde, 65 F. Supp. 2d 567 (S.D. Tex, 1999). Specific intent is defined at common law as follows:

The intent to accomplish the precise criminal act that one is later charged with. General intent is defined as "the state of mind required for the commission of certain crimes not requiring specific
results in system degradation is required to hold a person punitively accountable for violating the regulation. Despite the recognition of threats to the GIG, AR 25-1 incorporates the permissive access to Internet doctrine found in the JER.\(^4\) This permissiveness includes, personal “brief Internet searches,” without providing any further parameters as to the meaning of the limitation.\(^5\)

Air Force Instruction (AFI) 33-129, *Communications and Information: Web Management and Use*, is the Air Force’s counterpart to AR 25-1.\(^6\) Like AR 25-1, it provides a framework for access, modeled on the JER.\(^7\) Also, like its Army counterpart, AFI 33-129 provides a non-inclusive list of inappropriate use. This list is broader than AR 25-1 as it also prohibits modifying or altering the network operating system or system, and permitting an unauthorized individual to access a DOD computer system. However those two examples are

intent. General intent usually takes the form of recklessness (involving actual awareness of a risk and the culpable taking of that risk), or negligence (involving blameworthy inadvertence).”

*Id.* at 571 (citing *BLACK’S LAW DICTIONARY* 813 (7th ed. 1999)).

\(^4\) AR 25-1, para. 6-1.d(1) (“The Joint Ethics Regulation, Section 2-301, serves as the basis for Army policy on the use of telecommunications and computing systems. Users will abide by these restrictions to prevent security compromises and disruptions to Army communications systems.”).

\(^5\) AR 25-1, para. 6-1.e. The regulation states the following:

Authorized use includes brief communications made by DOD employees while they are traveling on Government business to notify family members of transportation or schedule changes. They also include personal communications from the DOD employee’s usual workplace that are most reasonably made while at the work place (such as checking in with spouse or minor children; scheduling doctor and auto or home repair appointments; brief Internet searches; e-mailing directions to visiting relatives). Such communications may be permitted, provided they—

1. Do not adversely affect the performance of official duties by the employee or the employee’s organization.
2. Are of reasonable duration and frequency, and, whenever possible, are made during the employee’s personal time, such as during lunch, break, and other off-duty periods.
3. Are not used for activities related to the operation of a personal business enterprise.

*Id.*


\(^7\) See id. para. 2.1, which states: “Appropriate Use. Government-provided hardware and software are for official use and authorized purposes only. Appropriate officials may authorize personal uses consistent with the requirements of DDOD 5500.7-R, *Joint Ethics Regulation (JER)*...”

*Internet Access from Government Information Systems* 191
prohibited in other regulations. Moreover, AFI 33-129 is unique in prohibiting the use of measures to circumvent blocked sites or other security systems.  

IV. COURSES OF ACTION

There are at least four possible courses of action to effectuate a change in the current paradigm of almost-open Internet access. The DOD can draft a new regulation (or series of regulations) limiting access to the Internet through government information systems. Such a regulation would be divorced from the JER, but the JER would, in turn, require modification to section 2-301.

A second course of action is to have local commanders recognize the inherent risks of the current paradigm, preempt the JER and draft lawful orders applicable to the commander’s respective installation, command, or vessel. In the legal rubric of lawful command, it is, of course, possible for the President or SECDEF to issue a lawful command limiting Internet access through government information systems. This course of action could occur at a far more rapid rate than issuing a regulation but would come at the cost of denying full input from the services, combatant commands, and field agencies.

A third course of action would be to draft a new regulation, but while the process of drafting, input, and promulgation is occurring, permit local commanders to issue lawful orders. This course of action is essentially a hybrid of the prior two. Finally, a fourth course of action is to do nothing, and permit the JER and other service regulations and user agreements to regulate internet access through government information systems.

A. Lawful Order

Historically, the most immediate means of effectuating an enforceable policy change has been the issuance of a lawful order from a command authority. While lawful orders are generally issued by officers commanding installations or vessels, the President, followed by the SECDEF, are the two highest command authorities. They are

78 Id. paras. 2.2.1-2.2.14 list prohibited actions. Para. 2.2.9 prohibits attempts to “circumvent or defeat security or modifying security systems without prior authorization or permission (such as for legitimate system testing or security research).”

79 The basis for this construct is deeply rooted in American Constitutional jurisprudence. See, e.g. 10 U.S.C. §§ 111, 113 (2006); Martin v. Mott, 25 U.S. (12 Wheat.) 19 (1827) (authority over all military forces under the President’s constitutional status as commander in chief); Little v. Bareme, 6 U.S. (2 Cranch.) 170 (1804) (presidential authority over all service members not unlimited but very broad).
constitutionally empowered to issue orders which have a service-wide effect.\(^8^0\)

In terms of hierarchy and reach of authority, the three Service Secretaries, four commissioned chiefs of their respective services, and the combatant commanders follow.\(^8^1\) The authority to issue a lawful order descends to the lowest command level.\(^8^2\) Depending on the service, location, and chain of command, the level of authority may simply be whoever is of highest rank in a given chain.\(^8^3\) But, only the President and Defense Secretary have the ability to directly order the entire Department to comply with a policy.\(^8^4\)

The UCMJ, Article 92, governs the punitive nature of lawful orders. The essential attributes of a lawful order include: (1) issuance by competent authority—a person authorized by applicable law to give such an order; (2) communication of words that express a specific mandate to do or not do a specific act; and (3) relationship of the mandate to a military duty.\(^8^5\) Orders are generally presumed to be lawful, and it is for a judge to decide whether this is the case.\(^8^6\) An

\(^{80}\) SECDEF may issue a general order which binds all service members (and by implication all civilian federal employees of the Department), notwithstanding that directives, regulations, and instructions are almost always conveyed in a specific format. See, e.g., United States v. Brown, 25 C.M.R. 20 (C.M.A. 1957); United States v. Snyder, 4 C.M.R. 15 (C.M.A. 1952).


\(^{82}\) See United States v. Voorhees, 16 C.M.R. 83, 96 (C.M.A. 1954) (“A general order or regulation is lawful if not contrary to or forbidden by the Constitution . . . an Act of Congress or the lawful order of a superior authority”).

\(^{83}\) See MCM, supra note 43, pt. IV, ¶¶ 14 & 16.

\(^{84}\) Id., pt. IV, ¶ 16(c)(1)(a); expressly gives to the SECDEF the authority to issue a punitive general order. A general order from the SECDEF may only be superseded by an order from the President or by a rescission from the SECDEF. No service or commanding general orders may contradict or modify the order. Unlike a directive or policy memo, an order is clearly applicable to all service members without distinction of position or rank (unless the order permits distinctions or exceptions based on legitimate service requirements).


\(^{86}\) United States v. New, 55 M.J. 95, 107 (C.A.A.F. 2001), quoting from Article 92:

The order must relate to military duty, which includes all activities reasonably necessary to accomplish a military mission, or safeguard or promote the morale, discipline, and usefulness of members of a command and directly connected with the maintenance of good order in the service. The order may not, without such a valid military purpose, interfere with private rights or personal affairs. However, the dictates of a person's conscience, religion, or personal philosophy cannot justify or excuse the disobedience of an otherwise lawful order.
order, in addition to showing its intent to regulate some aspect of behavior of servicemen, must state clearly whether it is punitive.\textsuperscript{87}

The issuance of multiple lawful orders across the DOD has two inherent difficulties rooted in law. Firstly, it is a fundamental due process right that DOD personnel have fair notice of the criminality of a prohibited conduct before being charged or convicted of an offense.\textsuperscript{88} If every military base, post, encampment, or station has its own separate set of rules, those particular rules have to be visible and understood by the persons falling within the jurisdictional reach of those specific rules.\textsuperscript{89} Even in a scenario in which major commands create their own independent rules, the issue of notice will exist, in part, because military personnel transfer from post to post. While the difficulty of providing notice is not insurmountable, it is far less difficult if the order is issued from the highest levels.

Secondly, one of the potential enforcement problems with commanders independently issuing orders in the absence of a regulation may be challenges based on the Fifth Amendment’s guarantee of “equal protection.”\textsuperscript{90} Rooted in due process, “equal protection” protects individuals from differences in treatment from a convening authority.\textsuperscript{91}

Within the services, different commanders may issue differing orders, with unique prohibitions. A violator of one order might seek to challenge a commander’s decision to offer non-judicial punishment or prefer charges for violating the order. While “equal protection” challenges might arise from the fact that each of the services (or, the major commands within each service) have different prohibitions against unofficial Internet access, the majority of these challenges would

\textsuperscript{87} The MCM reflects the fact that a myriad of regulations, instructions, and manuals govern virtually every aspect of military life, and that most of these issuances are not intended to establish the criminal offense of violating a lawful general regulation. See United States v. Nardell, 45 C.M.R. 101 (C.M.A. 1972); United States v. Hogsett, 25 C.M.R. 185 (C.M.R. 1958).

\textsuperscript{88} See, e.g., United States v. Tolkach, 14 M.J. 239 (C.M.A. 1982).

\textsuperscript{89} See United States v. Pope, 63 M.J. 68, 73-75 (C.A.A.F. 2007); see also Cole v. Arkansas, 333 U.S. 196, 201 (1948).

\textsuperscript{90} U.S. CONST. amend. V; see also Skinner v. Oklahoma, 316 U.S. 535 (1942). In Skinner, the Court held that “when the law lays an unequal hand on those who have committed intrinsically the same quality of offense . . . it has made as invidious a discrimination as if it had selected a particular race or nationality for oppressive treatment.”Skinner at 541 (citing Yick Wo v. Hopkins, 118 U.S. 356 (1886)); see also Gaines v. Canada, 305 U.S. 337 (1938).

\textsuperscript{91} For a good discussion of equal protection in military law see United States v. Courtney, 1 M.J. 438, 441 (C.M.A. 1976), and, most recently, United States v. Pauk, 66 M.J. 641 (A.F. Ct. Crim. App. 2008). In Pauk, the Air Force Court determined it was not a violation of equal protection if Air Force judges were non-tenured for a fixed term of service, while Department of the Army military judges and Coast Guard military judges served for fixed-tenure terms. The Navy-Marine Corps Court of Criminal Appeals determined similarly to the Air Force Court in United States v. Gaines, 61 M.J. 689 (N-M. Ct. Crim. App. 2005).
fail. "Equal protection" usually applies to constitutionally suspect classes of individuals who have historically suffered discrimination based on race, religion, or national origin. In 1981, the Court of Military Appeals (the predecessor to CAAF), in United States v. Means, determined that the rank or status of an individual could be a determining factor in a commander's decision to refer a military member to a court-martial as long as the status did not involve race, religion, national origin, or another protected factor.

Lawful orders may exist in the form of standard "user agreements," in which the user of government computers agrees not to engage in non-mission related web surfing. Clearly a standard "user agreement" will be an appropriate instrument to provide notice as to a prohibition against unofficial access to the Internet. But alone, arguably the user agreement is not enough to create a culture change in Internet access.

B. Regulations

Punitive general orders issued directly from the Secretary of Defense to the entire Department have been rare since the Goldwater-Nichols Act. This is because the Department adopted a means for projecting policies, regulations, and other rules to its service members and federal employees mirroring the Code of Federal Regulations.

The issuance of regulations to the services is a function of the executive branch, which mirrors the legal construct of issuing lawful orders but occurs as a defined process. However, in comparison to

---

94 Id, at 165. In Means, the Court determined that the commissioned officer status of an accused is a permissible factor in determining to refer a trial for courts-martial. The court held:

Even if appellant's officer status had been a principal factor—indeed, the decisive factor—in the convening authority's decision to refer the case to a general court-martial, appellant would still have no valid constitutional grievance. For the Government to make distinctions does not violate equal protection guarantees unless constitutionally suspect classifications like race, religion, or national origin are utilized or unless there is an encroachment on fundamental constitutional rights like freedom of speech or of peaceful assembly. The only requirement is that reasonable grounds exist for the classification used.

Id.
95 10 U.S.C. § 121 (2006). "The President may prescribe regulations to carry out his functions, powers, and duties under this title." Id.
posting an order, the drafting and issuance of regulations is time consuming because it involves the comments and concerns of the service departments, combatant commands, and agencies. On the other hand, published regulations which specifically prohibit unofficial Internet access from DOD computers are the optimum means of establishing a single department-wide framework for mitigating risks from malicious code. There are, of course, legal considerations before drafting and implementing such regulations.

As in the case of lawful orders, any regulatory changes which affect the conditions of employment will likely require negotiation with collective bargaining units. While localized orders prohibiting unofficial access to the Internet will, at most, require limited notice to collective bargaining units, a DOD-wide regulation may require negotiation with multiple collective bargaining units representing personnel.

A new regulation will also require other changes. Certainly, the adaptation of a new regulation will require ancillary amendments to other existing regulations such as the JER, and the Department of Defense Dictionary of Military and Associated Terms will have to be updated to include the term “mission use.”

Another consideration is which DOD agency should be responsible for drafting the regulation. A new regulation may be proposed and coordinated through several venues within the DOD. The Assistant Secretary of Defense for Networks and Network Integration (ASD/NII) is the DOD’s Chief Information Officer (CIO). The ASD/NII CIO is charged with the responsibility for protecting the DOD’s net-centric data. The commander, U.S. Strategic Command (USSTRATCOM), is charged with overall responsibility for GIG.

---

96 For a comprehensive overview on the drafting and promulgation of regulations, as well as amending current regulations, see generally U.S. DEP’T OF DEF. INSTR. 5025.1, DOD DIRECTIVES PROGRAM (Oct. 28, 2007) [hereinafter DODI 5025.1].

97 “Coordination with Unions Granted National Consultation Rights. DOD issuances containing substantive changes in conditions of employment, including personnel policies and practices and other bargaining unit matters that affect DOD civil service and non-appropriated fund employees, shall be forwarded to the appropriate unions for comment. . . .” Id. at Encl. 3, para. 7.h.

98 DODD 8320.02, supra note 1, para. 5.1.1.3, directs ASD/NII CIO to:

Develop the policies and procedures to protect Net-Centric data while enabling data sharing across security domains and with multinational partners, other Federal Agencies, and State and local governments in accordance with law, policy, and security classification, in coordination with the Under Secretary of Defense For Intelligence and the Under Secretary of Defense For Policy.
operations and network defense in coordination with the CJCS and other combatant commands.  

Joint Task Force Global Network Operations (JTF-GNO), a standing joint task force under the command of USSTRATCOM, is organized to protect and defend the GIG.  

Of the twelve doctrinally assigned tasks to JTF-GNO, the first is listed, "direct GIG NETOPS to ensure confidentiality, integrity, availability, and efficiency of the GIG infrastructure and information services."  

In 2004, SECDEF ordered the services, combatant commands, and field agencies to comply with USSTRATCOM directives on securing the NIPRNet and SIPRNet.  

At a minimum, a regulation must comprehensively and clearly articulate proscribed conduct. This conduct should include limitations on access to the Internet for official purposes only. It should also prohibit DOD personnel from engaging in other risky activity such as transferring DOD information on personal thumb-drives. It must also prohibit the use of software to by-pass technical blocking of websites. Finally, the regulation must educate personnel as to the importance of safeguarding government information systems.  

C. Hybrid Approach  

Because of the length of time it may take for the DOD to promulgate a new regulation, independent commands may draft lawful orders or local regulations designed to reduce the amount of unofficial internet traffic. The only difficulty, other than those enunciated above,

99 Joint Chiefs Of Staff, Joint Pub. 6-0, Joint Communications System II-20 (20 Mar 2006) [hereinafter JP 6-0]. The joint doctrine states, "USSTRATCOM has overall responsibility for GIG operations and defense in coordination with CJCS and combatant commands. CDRUSSTRATCOM is responsible for coordinating and directing DOD-wide CND. USSTRATCOM through its JTF-GNO component executes the DOD mission." Id.

100 See, e.g., id. at II-21-23; Cartwright, supra note 3, at 73.


Upon receipt, the military departments will organize to execute global network operations and network defense under the Service Headquarters assigned to USSTRATCOM. Defense agencies will align their global network operations and network defense capabilities to provide USSTRATCOM visibility and insight into network status. Military departments and agencies will respond to USSTRATCOM's orders and direction, allowing USSTRATCOM to defend the Global Information Grid.

Id.
is that commands may have to rescind orders if these conflict with the regulation.

D. Support from Other Jurisdictions.

While the issuance of regulations or orders limiting access to the internet for official use is important, guidance from federal and state courts, as well as administrative decisions should to be considered in the enforcement of rules. For instance, in *Eliserio v. United Steelworkers of America, Local 310*, the Eighth Circuit Court of Appeals, in overruling a lower court’s grant of summary judgment, found that the enforcement of rules against Internet misuse was arbitrary and could have occurred as a result of unlawful discrimination.

In *Thompson v. State Civil Service Commission*, the Pennsylvania Appellate Court upheld a county’s decision to terminate an individual’s government employment resulting from violations of the county’s computer use policies. Although part of the decision to terminate employment occurred as a result of the individual accessing sites containing nudity, evidence that the individual “surfed” the Internet for at least twenty to thirty percent of the workday was also a reason.

Decided by the Connecticut Supreme Court this year, *McCann v. Department of Environmental Protection* is the most compelling and relevant case to the issue of reducing risk through regulations on social behavior. McCann began his employment with the state government in 1985. Over time, the state issued McCann a laptop computer. In 1998, the state government issued a directive to its employees that government-issued computers were for “official and authorized business purposes.” The state informed its employees that

---

103 Eliserio v. United Steelworkers of Am., Local 310, 398 F.3d 1071 (8th Cir. 2005).
104 Id., at 1079. While the court found that five separate complaints of Internet misuse were made against the appellant, it also found that the appellant was the only employee disciplined by Firestone, the employer, in an eight-year period. Moreover, the appellant was not notified of any infractions for the first four complaints. Id.
106 Thompson, 863 A.2d. at 183.
108 Id.
109 Id. The policy stated:

All computer resources, including devices, programs, and data, electronic or hard copy, owned or leased by the State of Connecticut, and facilities of the State of Connecticut, which include but are not limited to the department, shall only be used for legitimate and authorized business.

104 Id.
violations of the directive could result in discipline including job termination. In 2001 and 2002, McCann’s supervisors reiterated the state directive’s prohibitions against unofficial use and articulated a “zero tolerance” policy towards violators.

In 2002, the state discovered McCann had downloaded a K-Mart commercial software package onto his computer after he brought his computer to a repair center. A supervisor verbally reprimanded McCann after this discovery. During an “upgrade,” in 2004, a Wal-Mart Internet commercial software program was found on a second state-issued computer used by McCann. Additionally, computer technologists discovered over 7,000 commercial web entries and a latent virus capable of degrading the state’s computer networks. Later that year, a third state-issued laptop computer used by McCann was infected after he accessed several unofficial websites.

The state notified McCann it had decided to terminate McCann’s employment based on numerous violations which placed the state’s information systems at risk. Because McCann belonged to a collective bargaining unit, he was entitled to an administrative hearing. The arbitrator determined McCann was given enough notice that his conduct violated state rules and the employment termination was justified. Important to this article’s advocacy was the arbitrator’s determination that “unauthorized use of [McCann’s] laptop...caused it to be infected with a virus that threatened the [s]tate's entire computer network, no small matter.”

McCann appealed to a state trial court, which ruled that the arbitrator failed to consider whether the state “offered McCann progressive discipline” and improperly excluded evidence of prior arbitrated agreements between the state and third parties who engaged in similar conduct, as well as the issue as to whether the state had disciplined employees for similar conduct. The trial court determined that the evidence did not support the arbitrator’s assessment of the risk to Connecticut’s state computer systems caused by McCann’s conduct.

The Connecticut Supreme Court reversed the trial court’s determination as to the arbitrator’s failure to include disputed evidence but agreed that the arbitrator could not have made the risk determination based on the quantum of evidence the state provided. However, the state supreme court upheld the arbitrator’s decision to support McCann’s employment termination and, more importantly, left open the prospect that conduct such as McCann’s, which created vulnerabilities

---

110 Id.
112 Id. at 8.
113 McCann, 952 A.2d at 46.
to malicious code, could be the basis for disciplinary action. This is precisely the construct which the DOD should adopt in enforcing regulations on unofficial Internet access.

V. CONCLUSION

One need only to look at the open source headlines and academic literature to understand the depth of the problem facing the DOD. These threats span a wide range, from the exfiltration of data to full scale denial of service attacks. As previously noted, a well-intentioned e-mail user within the DOD sent a link to an infected Internet game site. Two current nation-state adversaries, or their citizens, have repeatedly attempted to probe weak-points within the DOD and defense contractors. At least three weeks prior to the Russian invasion of Georgia, Russian government agencies, or its citizens, independently stepped up cyber attacks on Georgia. The potential for a terrorist strike against DOD information systems must be considered. The primary vector of attack will be through the Internet to the NIPRNet connection points. In essence, the threat to DOD information systems through cyberspace is very real, and a defense in depth is required to meet it. The defense should begin with social behavior, in essence, modifying the culture of permissive use, but include technical solutions as well.

It may be the case that commanders, judge advocates, and DOD personnel will view the implementation of a new regulation or series of orders designed to reduce the amount of Internet access traffic as a draconian measure. But, a decision to maintain the status quo and continue the permissive browsing of the Internet increases the risk of dangers ranging from exfiltration of data to a cyber “Pearl Harbor.”

Understandably, the DOD and its commanders possessing UCMJ authority may want to resist measures which will likely be detrimental to morale. Certainly, a DOD-wide regulation should exempt deployed servicemembers, as well as personnel assigned to naval vessels operating at sea, because an alternative private means to access the Internet is unlikely to exist in austere locations. It is also understandable that commanders and departmental leaders will worry

114 Id.
about recruiting and retention, both for uniformed personnel and the civilian workforce, and therefore not wish to create a policy limiting use. One solution may be for the acquisition of Internet connected computers in cafes and kiosks not connected to the .mil network. This solution, while outside the scope of this article, should be considered for later advocacy.

Social behavior, even in the armed services, cannot change without education and the development of policy. This is true, particularly, where the behavior to be limited is predicated on the assumption that no harm is caused by it. But the risk factors involved in unfettered internet access are too great to ignore. As a result, the DOD, or, in the absence of DOD action, responsible commanders with the support of their military legal community, should lay the groundwork for changing the paradigm.
SUBJECT: Protection of DoD Information Systems

(c) DoD 5500.7-R, Joint Ethics Regulation
(d) Chapter XX of title 10, United States Code

1. PURPOSE

This directive:

1.1. Establishes policy for eliminating the high level of unofficial use of Department of Defense (DoD) information systems, including systems used to access NIPR, SIPR, and other information systems.

1.2. Assigns responsibilities, and prescribes procedures for the Military Departments, Combatant Commands (COCOMS), and agencies regarding the use of DoD information systems and reporting of violations of this instruction.

1.3. This instruction does not supplant or replace other regulations, policies, and instructions governing the use of government property or the protection, handling, and use of classified information.
2. **APPLICABILITY AND SCOPE**

This directive applies to:

2.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, and all other organizational entities in the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.2. The Coast Guard when it is not operating as a Military Service in the Department of the Navy by agreement with the Department of Homeland Security; and the Commissioned Corps of the United States Public Health Service (USPHS) and the National Oceanic and Atmospheric Administration (NOAA), under agreements with the Department of Health and Human Services (hereafter referred to collectively as "Other Uniformed Services"). The term "Military Services," as used herein, refers to the Army, the Navy, the Air Force, the Marine Corps, and the Coast Guard; and their respective National Guard and Reserve components. The term "Uniformed Services" refers to the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Commissioned Corps of the USPHS, and the Commissioned Corps of the NOAA.

2.3. DoD-owned information systems (IS) and DoD controlled IS operated by contractors or other entities on behalf of the DoD that receive, process, store, or display, or transmit DoD information, regardless of classification or sensitivity, consistent with Reference (x).

3. **DEFINITIONS**

Terms used in this directive are defined in Enclosure 1.

4. **POLICY**

Commensurate with the determination that Global Information Grid (GIG) is a war-fighting domain, it is DoD policy to protect the confidentiality, integrity, and availability of classified and unclassified,
but protected information, located on the GIG; and, to ensure the DoD components have complete access to the GIG per mission needs.

4.1. Internet traffic from DoD information systems has exponentially increased each year, creating challenges to unhindered GIG access. These challenges include risks posed by malicious code, as well as clogged pipelines. Furthermore, it is estimated that in FY 2007 at least 60% of all internet traffic originating from DoD information systems is accessed for unofficial (non-mission related) purposes.

4.2. DoD information systems are also placed at risk through the interface of private computer systems and information transfer technologies.

4.3. With the growth and increasing complexity of malicious code, unofficial use of the DoD information systems on the NIPRNet must be curbed to the maximum extent practicable.

4.4. Unofficial use includes, but is not limited to: accessing internet sites not directly related to military duty, “web-surfing,” accessing non DoD web-mail from DoD information systems, and, the transfer of official files from DoD computers to non-DoD computers without the prior authorization of the first general officer in a chain of command or civilian equivalent. It also includes the use of privately owned (non-DoD appropriated) information transfer technologies such as personal thumb-drives, on DoD information systems.

4.5. This directive exempts DoD personnel deployed to the CENTCOM AOR or other deployed regions, DoD personnel aboard naval vessels or space vehicles as a local commander may direct.

5. RESPONSIBILITIES

5.1. The Commander, United States Strategic Command (CDRUSSTRATCOM) shall:

5.1.1. Draft and implement policy to limit the unofficial access to the internet through DoD information systems, consistent with the authority to operate and defend the GIG.
5.1.2. Test and evaluate scientific and technological methods for limiting unofficial access to the internet.

5.1.3. In cooperation with the Assistant Secretary of Defense for Networks and Network Integration, draft and develop enforceable policy to hold accountable DoD agencies and personnel who place the GIG at increased risk.

5.1.4. Monitor compliance with DoD policy limiting the use of access to internet for official purposes and make a quarterly report to OSD.

5.1.5. Develop policy for investigating Cyber intrusion and malicious code events.

5.1.6. Report to the Secretary of Defense the results of investigations, the availability of the GIG, and DoD compliance to this directive.

5.2. The Assistant Secretary of Defense for Networks and Network Integration (ASD/NII) shall:

5.1.1. In cooperation with USSTRATCOM, draft and implement policy to limit the unofficial access to the internet through DoD information systems.

5.1.2. In cooperation with USSTRATCOM, monitor compliance with this instruction

5.3 The General Counsel to the Office of the Secretary of Defense shall:

5.3.1. Modify DoD 5500.7-R, the Joint Ethics Regulation, to comport with this policy, and modify other departmental regulations as needed.
5.4. The Secretaries of the Military Departments shall:

5.4.1. Draft and implement punitive regulations to curb the use of DoD information systems to access the internet for unofficial purposes.

5.4.2. Modify existing service regulations to comport with this directive.

5.4.3. Educate members of their respective services as to the inherent dangers posed by internet access from DoD information systems.

5.4.4. Support CDRUSTRATCOM or the designated agency within the COCOM on all cyber intrusion investigations.

5.5. The Chairman of the Joint Chiefs of Staff shall:

5.5.1 Develop or modify joint doctrine and associated joint tactics, techniques, and procedures for the GIG and ensure the compatibility of the Chairman of the Joint Chiefs of Staff Instructions with this regulation.

5.6. Authorized Users of DoD information systems shall:

5.6.1. Access the internet only for mission related purposes as defined in enclosure (A)

5.6.1. Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

5.6.2. Use only DoD issued hardware and software for transferring electronic data.

5.6.3. Report suspected violations of DoD policy to an immediate supervisor, or if not practicable, to the next highest level.

6. EFFECTIVE DATE

This Instruction is effective immediately.
ENCLOSURE

DEFINITIONS

E1. Global Information Grid (GIG)

   E1.1 The globally interconnected, end-to-end set of information
capabilities, associated processes, and personnel for collecting,
processing, storing, disseminating and managing information on
demand to warfighters, policy makers, and support personnel. The GIG
includes all owned and leased communications and computing systems
and services, software (including applications), data, security services,
and other associated services necessary to achieve Information
Superiority. It also includes National Security Systems as defined in
section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all
Department of Defense, National Security, and related Intelligence
Community missions and functions (strategic, operational, tactical, and
business), in war and in peace. The GIG provides capabilities from all
operating locations (bases, posts, camps, stations, facilities, mobile
platforms, and deployed sites). The GIG provides interfaces to
coalition, allied, and non-DoD users and systems.

   E1.2. Includes any system, equipment, software, or service that
meets one or more of the following criteria: transmits information to,
receives information from, routes information among, or interchanges
information (DODD 8100.1).

E3. NIPRNET. Non-Classified Internet Protocol Router Network. A
computer network for unclassified, but sensitive information supporting
the DoD (JP 6-0).

E4. SIPRNET: Secret Internet Protocol Router Network. The
worldwide SECRET-level packet switch network that uses high-speed
internet protocol routers and high-capacity Defense Information
Systems Network circuitry (JP 6-0).

E5. UNOFFICIAL USE: Use which does not relate to the functions or
necessities of DoD personnel or mission sets.
SECDEF GENERAL ORDER #1

From: Honorable Robert M. Gates
SECDEF
To: 
Date:

1. Statement of Military Purpose and Necessity: The amount of DoD network resources devoted to internet and web traffic has increased exponentially over the past several years. Analysis indicates the majority of this traffic occurs for non official purposes. Not only does this drain resources better devoted to the DoD mission, but each connection exposes DoD networks to additional risk. The aggregate risk across DoD associated with this unnecessary exposure is substantial and unacceptable. DoD personnel have long operated on the assumption that using DoD network resources for personal purposes was cost free. It is not. DoD networks must be reclaimed for official use only.

2. Prohibited Activities:

   a. Use of DoD computers and/or networks to access the internet and world wide web resources if the intended purpose of that access does not serve an official purpose. Examples of prohibited activities include recreational web surfing; personal use of social networking, gaming, and shopping sites; and the use of peer-to-peer networks.

   b. The connection of any personal electronic device or media to DoD computing equipment.

   c. Connection from DoD networks to any web-mail services hosted outside the .mil domain.

   d. The transfer of non-public DoD files to home systems; the transfer of files from home system back to DoD systems.

3. Email: This order does not place additional restrictions on whether DoD personnel may send personal email from DoD-supplied email accounts beyond what is already regulated through DoD Directive 5500.7, dated 30 August 1991 (Joint Ethics Regulation), or prohibited by other laws and policy.

4. Punitive Order: Paragraph 2 of this General Order is punitive. Persons subject to the Uniform Code of Military Justice may be
punished thereunder. Civilians serving with or employed by the Armed Forces of the United States may face adverse administrative action for violation of this General Order.

5. Individual Duty: All persons subject to this General Order are charged with the individual duty to refrain from any use of DoD computers and networks in a manner that unnecessarily (other than an official purpose) connects them through the Internet/World Wide Web to non DoD systems. Questions regarding whether a particular use serves an official purpose should be referred, in advance, to a supervisor or commander.

6. Unit Commander Responsibility: Unit commanders and supervisors are charged to ensure all personnel are briefed on the prohibitions and requirements of this General Order. Commanders and supervisors are expected to implement monitoring programs to assist with enforcing this order.

7. Effective Date: This General Order is effective immediately.

8. Expiration: This general order will remain in effect until rescinded, waived, or modified.

9. Waiver Authority: Authority to waive or modify the prohibitions of this order is delegated to the first Flag, General Officer, or SES in an individual’s chain of command or supervision. Any waiver or modification must be documented in writing and indicate the specific factors that justify the waiver or modification.