Gigabits, Gateways and Gatekeepers: Reliability, Technology and Policy

John C. Wohlstetter

Do not quote without permission of the author.

Columbia Institute for Tele-Information
Graduate School of Business
809 Uris Hall
Columbia University
New York, New York 10027
(212) 854-4222

GIGABITS, GATEWAYS AND GATEKEEPERS:

RELIABILITY, TECHNOLOGY AND POLICY

John C. Wohlstetter
Director - Technology Affairs
GTE Corporation

Quality and Reliability of Telecommunications Infrastructure
Columbia Institute for Tele-Information

April 23, 1993

Introduction

Telephony met Information Age reality on January 16, 1990. It was AT&T's misfortune to lose over 50 percent of its network capacity when a single-bit "soft-glitch" cascaded through 114 SS7 adjunct processors in its 4ESS network--in 20 minutes. (AT&T's SS6 traffic survived.) Software control over public-switched networks became clear to all.

Taken even alone, that increasing dependence is cause for concern. Magnifying the danger, however, are the proliferation of diverse, computer-controlled customer premises equipment and, more significant, of increasingly interconnected, separately-managed *networks*. Some of these issues were addressed in the FCC's recently-adjourned Network Reliability Council. The Council's solid work--and the FCC's--have made a constructive contribution to improving network reliability, and both bodies deserve commendation.

But some risks to reliability were neither fully resolved by the Council nor by the FCC itself. Today, I propose to talk about one: policing software access to networks.

I. The Emerging Meta-Network: From Physical to Virtual Tele-Worlds

It is now common currency to call our public-switched network fabric a "network of networks," with linkage at both the hardware and software levels. True, even in the Age of Ma Bell there were hundreds of independent company telephone networks, interconnected to the Bell System; but in those days we thought of the collective whole as a unitary "national public-switched telephone network." It was, essentially, Bell-driven: based on Bell technology, under Bell standards and pretty much playing by Bell rules. Today, physical network segmentation is a much broader phenomenon, in that it is accompanied by increasing software inter-dependence: we will find ourselves dealing with the consequences of this revolutionary paradigm shift into the next century.

A. Heterogeneous Hardware: LAN-CAP-IXC-Cell-LEC-LAN. Even the nation's first baby-boomer President can remember a time when phones came in three colors: basic black, midnight-black and pitch-black. There was another side to this: you could have asked anyone at AT&T. what kind of equipment was connected to the network, and you-would have been told: black phones--by Western Electric. Of course, you could also have simply looked at the phone in your den.

Not so any more. Neither AT&T, nor the local exchange telephone companies, nor *anyone else* can tell you what is connected to the public network fabric today. What goes on behind the network demarcation point is, literally, *none of the network provider's business.* Desktop computers, mainframes, PBXs, FAX machines, hand-sets, you name it--provided by hundreds of manufacturers scattered around the globe.

B. Seamless Software: My Bits...Your Bits...OUR Bits? In a certain sense, software represents a technological Faustian bargain: in exchange for a quantum leap in network capabilities--control, flexibility, new services--there is a troublesome price to be paid: the increased vulnerability of software-based networks. This vulnerability arises from four fundamental characteristics of network software: (1) it is *global*; (2) it is *programmable*; (3) it is *accessible*; and (4) it is *fragile*.

"Global" means that software represents a unitary logical overlay of dispersed physical network hardware. Thus, a single-point *logical* failure can, as happened to AT&T, cascade through dispersed physical nodes. *Hardware fails independently; no single-point hardware failure could have disabled half of AT&T's nationwide network capacity.*

"Programmable" means that software code can alter the way network hardware runs: whereas picking up the telephone simply means closing an electric circuit between the phone and the central office, sitting at a PC the user can *re-direct network assets.* Members of the hacker group "Legion of Doom" did just that a few years back, forwarding 911 calls in a Bell Operating Company's network to a dial-a-porn service.[1]

"Accessible" means that network assets are becoming more widely available, per Open Network Architecture. Service providers are gaining access to network software, and pressing for complete control over the services they derive from telephone networks.

And "fragile" means that when software "breaks" it is not easy to "fix." It took AT&T two weeks to find the faulty code that brought its SS7 network down. They found an AND condition in place of an OR condition--out of *millions of lines of code.* Looking for this stuff is not made any easier in that at the start of the search you do not know what kind(s) of logical code error(s) you are looking for.

Now, add in multiple networks and multiple providers. The rash of SS7 network crashes in the summer of 1991 was caused by faulty code in an update of SS7 software provided by DSC Corporation; companies not using DSC code were spared. It is only a matter of time before faulty code crosses a network gateway--to crash someone *else's* network.

C. Gateway to the Stars: A "Virtual Bridge" Entrance? We will have more to say about this later, but for now simply note that at the entrance to each provider's network is a "gateway" that establishes, so to speak, the "rules of the road" for accessing the network. *Inherent in the nature of software is the ability--unless controls are effective--to reach across gateways and control the operation of distant networks.*

Technology is transforming today's networks: the central office switch is a digital computer; every desktop workstation or home PC is potentially a digital switch. Thus, transmission, switching, computer processing and memory management functions, to date essentially distinct operations, are now being weaved into a web of interconnected computing/communication networks.

The merger is a product of the combination of digital electronic hardware and software: dispersed physical assets are controlled by a unitary overlay logical network. The logical overlay not only controls the operation of the physical network *infra*structure, it creates a functional *super*structure; access to network software logic enables both network providers and network users to define new network configurations--*virtual* networks. (In techno-parlance, "virtual" denotes the logical, software-defined equivalent of physical hardware functionality.)

II. Regulating Reliability: From Hippocrates to Pangloss?

When the nationwide network was primarily entrusted to AT&T--Theodore Vail's "one system, one policy, universal service"--Ma Bell guarded it as a national treasure. Any act that could conceivably bring harm to the network was simply *verboten*. Subscribers either took service on AT&T's terms, or wrote letters. This began to change with equipment deregulation.

A. Harmless Hardware: The Legacy of Part 68. When the FCC began weighing rules to govern interconnection of equipment to telephone networks AT&T, as part of its case in opposition, warned that if defective equipment were connected harmful voltage--potentially lethal--could be sent over the network. Callers injured during a thunderstorm by lightning voltage could attest that the danger was not merely hypothetical.

Once it became clear that interconnection was inevitable, the debate shifted to what safeguards should be adopted and who would have responsibility. Equipment vendors denied that their equipment would cause harm and placed responsibility on the network provider. In the end, the FCC adopted Part 68, providing for interconnection on demand for equipment registered under Part 68. In doing so, the FCC in effect followed the precept of the legendary father of medicine: "First, do no harm."

But Part 68 also enshrined another precept, for once and for all: beyond the network demarcation point--in most cases, an RJ 11 modular jack--*what the customer does on the premises is--at least, generally--no one else's business.*

B. Safe Software: The Promise--Hope?--of ONA. Open Network Architecture represents, essentially, the software equivalent of hardware interconnection. Just as the physical assets of the network were opened up, now the logical assets are opening to outside access. But there is a crucial difference: hardware access means passive acceptance of network service; software access means potential *control* over network assets. The customer who merely connects equipment under Part 68 cannot re-direct 911. Now this is changing--radically.

ONA is opening networks up to a potentially vast pool of users. With more people enjoying access to network features and with more of the network's innards (software primitives) being made available, opportunities for abuse--accidental and well as premeditated--of network assets will clearly increase, unless adequate counter-measures are implemented. Moral: Unless we, like Voltaire's Pangloss in *Candide*, believe this "the best of all possible worlds" we need the equivalent of a software Part 68.

III. Reliability and Responsibility: Am I My Tele-Brother's Tele-Keeper?

As I briefly noted above, network entrances--"gateways"--represent the ports of call for information traveling through the network fabric. Increasingly, in a digital environment, all that the gateway will mark will be bits--an increasingly seamless, endless digital bit stream. Not voice; not data; not image; not video. Just...BITS.

A. Gateways: Toll Booths on the Information Super-Highway. Everyone who travels America's highways knows that, sooner or later, there will be tribute rendered to Caesar. The toll booth is as much an image of the automobile age as are tail-fins. A network gateway can represent the same thing on Vice-President Gore's Information Super-Highway: collection of necessary tribute to support the fabric. The toll paid is, of course, for exercising the right of access to network facilities. But is this enough?

B. Gatecrashers: Digital Dillingers, Accidental Tourists. We each have our own list of whom we consider yesterday's heroes. Some of mine: Alexander Graham Bell; Theodore Vail; Edwin Armstrong; Claude Shannon; John von Neumann; Robert Noyce.[2] But how many of *these* names ring a bell: Robert Tappan Morris; Pengo; Frank Darden?

Morris launched the INTERNET "worm" on its not-so-merry way one fine day in 1988, crashing 6,000 computers and causing, by one estimate, $98 million in lost computer time.[3] Pengo was a member of the West German hacker club, KAOS, which in 1987 - 1988 prowled through confidential Pentagon databases in search of information for the KGB.[4] And Darden was a member of the teen hacker group "Legion of Doom," whose re-routing of Bell South's 911 service was a major tele-caper. The first was negligent; the second, a spy; the third, a malicious prankster. *They* are part of the Information Age future. And *we* had best learn how to deal with them.

In addition to the "digital Dillinger" threat there is the problem of the "accidental tourist." The SS 7 failures that crashed several local exchange carrier networks in the summer of 1991 were caused by a faulty software upgrade supplied by a single vendor of SS 7 software. That vendor supplied SS 7 software for 100 Signal Transfer Points (STPs) in several carrier networks; *57 STPs had the defective code installed.*[5]

According to the FCC's own report on the STP failures, the outages were caused by a confluence of three factors: (1) *three bits* of faulty code supplied by the vendor; (2) a "triggering event"; and (3) weekday "busy-hour" call overflow between 11 AM and 2 PM.[6] The triggering events differed with each outage, but the common result was call congestion overflow on STP links. *The vendor did not fully test the update code.*[7] And even had the code been thoroughly tested, the vendor conceded that it could not have simulated "a complete range of potentially contributing trigger sources."[8]

C. Gatekeepers: Toll Collectors or Bit-Bouncers? This is, so to speak, "where the rubber meets the road." This is where a software Part 68 would have to fit. Just as standards were adopted for registering hardware that is connected to the public network fabric we now need *software* standards.

Fixing responsibility for "bit-bouncing" on gatekeepers is not an abstract issue. Last session of Congress saw legislation introduced that would have imposed financial penalties on carriers whose networks went down. The measure of damages would have depended upon the scope and duration of the outage and the degree of fault assigned the carrier.[9]

Now, suppose that I tape my password to my PC, or that my password is "password." Someone logs on (either on premises or remotely) to my PC, and after entering the correct log-in name and password, is *for all intents and purposes a legitimate user.* Newly legitimized, the hacker now dials out through the office PBX and calls a network database in California. Bypassing security at the database--let us say, by stealing passwords as Pengo did when entering some 400 military networks--the caller now sends to the database a little surprise: *Michaelangelo.* And not a video of the Sistine ceiling.

OK, if your distant database is "zitzed out," who pays? *I* was negligent. Should Pacific Bell pay? As a common carrier with no right to control message content, PacBell merely carried bits over its network. *We need "rules of the road" which enable us to trace damage to the source and fix responsibility accordingly.*

Gateway policing is a sfftware security issue that has been examined by the National Security Telecommunications Advisory Committee (NSTAC), a CEO-level body that advises the National Security Council.[10] In a 1992 report, NSTAC recommended that industry and government cooperate to develop uniform standards for public network--and inter-network--security.[11] The report stated that while "it is a leap to connect" collusion among hackers" to "group intent to take-down the PSN" a "serious **potential** threat exists: a resourceful adversary starting with the hacker information base."[12]

That base includes electronic bulletin boards--some with multi-level security so that top hackers can limit access to their purloined information.[13] More worrisome, the report notes a shift in hacker motivation towards "financial gain."[14] This contrasts with the traditional authority-defying motive. Finally, hackers have become more skillful at circumventing password protection and at defeating dial-back modem techniques.[15]

The report recommends possible action in six areas: (1) control of network element access (*e.g.*, smart cards); (2) appropriate "level of suspicion" between networks (to isolate "weak links"); (3) recovery from software or database damage; (4) software memory partition and damage isolation; (5) network element analysis (*e.g.*, audit trails); and (6) future architecture planning.[16]

D. Customers: A Tele-World "Reasonable User" Standard? Last month a Maryland federal court decided a suit brought by Jiffy-Lube International, a small business, against AT&T.[17] Jiffy-Lube sought reimbursement of $55,000 lost to a "call-sell" operator who successfully dialed into Jiffy-Lube's PBX. Calls were then made to the usual far-away watering-holes, at Jiffy-Lube's expense. As articles in several national magazines have recently detailed, such "rogue resale" is on the rise.

Jiffy-Lube's claim ran head-on into a contractual provision of AT&T's tariff, which held the "customer" liable for misuse. In granting summary judgment to AT&T the Court gave short shrift to Jiffy-Lube's claim that AT&T should be held liable despite the tariff provision, for carrying the hacker's call into Jiffy-Lube's PBX. Jiffy-Lube's case was not helped, one suspects, by their choice of password: "Lube." Nothing like originality.

Query: Given Jiffy-Lube's choice of password, would Jiffy qualify as a "reasonable customer?" Given widespread news reporting of hackers and call-sell rip-off artists, are not subscribers, with respect to their own network vulnerability, on "notice"--a legal term of art meaning what you *should* know, regardless of whether you *actually* do know? Should a "reasonable user" standard be more lenient for Aunt Tillie than for a Local Area Network manager? And if Aunt Tillie's teenager hacks from his PC, should she spot it?

E. Soft-Access: Who Gets to Play the Wizard?

Access to network software, the essence of ONA, can be understood at two distinct levels: (1) *user-level* access; and (2) *system-level* access. "User access" means the ability to avail oneself of network service applications; "system access" means the ability to *manage* network operations, *i.e.*, to change the way the network runs. A hacker's prime goal, upon entering a new system, is to become a "super-user"--with all the powers of the system administrator (also called "administrative privilege").[18]

System-level *access* thus means system-level *control.* As ONA service users--both competing network service providers and major users--penetrate deeper into the core networks of telephone companies, their access moves closer to the system-level line. They desire full software-based control over their network services, incorporating comprehensive functionality.

In pressing for deeper ONA, the November 1991 petition of the Coalition for Open Network Architecture Parties (CONAP) called for a "modular, transparent architecture."[19] Included in their concept of Open Systems Interconnection (OSI) is "access to system-level programs and commands."[20] They acknowledge the need for network security:

> No one would argue that the nation's public telephone network should be left "wide-open" to anyone who might choose to wander into it; a high level of network security is an essential element of any public telephone network design.[21]

CONAP pointed to the "extreme success" of the open architecture adopted by IBM in the personal computer market. By analogy, they suggested that the telephone network should, increasingly, work just like a PC.[22] *Precisely.* Ask anyone whose hard disk has been "totaled" by some rogue program how safe computers are. In terms of economic impact, it is one thing to crash PCs and quite another to crash a central office switch.

It should also be noted that while IBM's open architecture has made IBM-compatible computers the most marketable, it has also made them the prime targets of the hacker community.[23] Apple's closed architecture has made its machines harder to penetrate. In noting this I do not intend argue against open architecture *per se*, but merely to note a *collateral* cost of open access.

In such an environment, software "partitions" may be today's key line of defense. Hackers have, however, proven notoriously skillful at circumventing software-based defenses. Ultimately, hardware defenses may prove necessary.[24] *If in the meantime, network providers are required to open their system-level access, liability for harm should be shared.* One telecom consultant associated with the FTS-2000 contract stated:

> (N)etworks are just an extension of the PCs, and virus protection should really begin at the terminal, regardless of the type of network you are using. If you don't stop the virus from getting into your PC, you won't keep it out of your network.[25]

For its part, the FCC has acknowledged that network reliability and integrity represent considerations associated with efforts of various interests to gain deeper software access to telephone networks.[26] Critical as part of such an assessment is apportionment of responsibility for harm done, just as with the equipment registration program.

IV. Cyber-Culture: Who Rules Cyber-Space?

Marshall McLuhan's "global village" is here--lest *anyone* doubt this a hacker in Melbourne, Australia was arrested in 1991 for breaking into American nuclear research and space agency computers, shutting down one Norfolk, Virginia NASA computer for 24 hours, altering and deleting data.[27] The village has a name: INTERNET, and already numbers millions of individual users. Streams of electrons and photons cross global network paths at warp speed. A New Yorker and a Malaysian communing via E-mail may share more in common than either does with their next-door neighbor. Electronic communities do not occupy land; they occupy what Lotus 1-2-3 founder Mitch Kapor calls "cyber-space." This did not signify much when telephone networks were radically different from their computer cousins. It does matter today. A new "Cyber-Culture" has emerged. For a moment, let's re-trace its roots.

Historically, telephone and computer industry access/security cultures were diametrically opposite. For a century telephone networks were closed systems, accessible by users almost exclusively for garden-variety voice communications usage. As recently as 1956, the old Bell System tried (ultimately unsuccessfully) to prevent customers from attaching a cup to the telephone, designed merely to allow users to converse privately in the presence of others (the "Hush-A-Phone" device). Deregulation, divestiture and their twin offspring, equal interconnection and open access to network functionality, have radically altered the telephone industry culture.

Computing culture originally moved towards openness. In the early-1960s computer use spread from a select few to university science campuses. Student programmers embraced a code of unbounded openness; computing creativity would be fueled by maximizing free access to systems and by programmers sharing their creative work with others in the computer community. The original cult of the computer hacker had as its hero the student prankster who would leave a humorous message on someone else's presumably inviolate machine; hacking was also a way to help de-bug program code.

Three 1980s phenomena transformed the open computer culture. First, the explosion of the computer market, triggered by the success of the PC, made software vastly more commercially valuable than ever before, and thus in need of protection from damage and piracy. Second, the rise of the malicious hacker, with his arsenal of "viruses," "worms," "time bombs," "logic bombs" and "Trojan Horse" programs,[28] made intrusion no longer the prankster's harmless hi-jink. Access became a double-edged sword. And third, the rise of networking radically leveraged--for worse--the vulnerability of computers.

In a 1991 report, the National Research Council, operating arm of the National Academy of Sciences, appraised the risk of "soft-terror":

> The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb....*To date, we have been remarkably lucky* . . . . (A)s far as we can tell, there has been no systematic attempt to subvert any of our critical computing systems. *Unfortunately, there is reason to believe that our luck will soon run out.*[29]

Ironically, *it was just as the telephone network was being opened up via Open Network Architecture that the computer world began to re-examine its own culture after the INTERNET debacle.*

A. Cyber-Follies: 800, 900, 911 and 976. Mass announcement numbers pose hazards that network designers never anticipated--indeed, even if they did it is doubtful if network economics would permit deployment of vast excess capacity that lies largely unused. This may change when we enter our Fiber Future, but until then it is a live issue.

In 1992, call-ins for tickets to hear music icon Garth Brooks jammed two local phone networks. One case was no laughing matter: a woman claimed that she could not reach 911 when her husband had a heart attack. Whether help would have arrived in time even with 911, we cannot say.[30] But the message is clear: 911 access must be safeguarded. The FCC has already acknowledged as much when it prevailed upon Pepsi to withdraw an 800-number call-in for the 1991 Super Bowl--on the eve of Desert Storm.

B. Cyber-Punks: Michaelangelo *Ex Maleficia.* Every time I sit at my PC I thank the Lord that "Saddam don't know software." So far, at least that we know, terrorists seem to prefer buckets of blood to evil electrons.[31] Most hacking to date has been mere "cyber-pranks." *We cannot assume that we will continue to enjoy virtual immunity from software invaders who intend--and know how to inflict--real damage.*[32] Knowledgeable programmers who examined Robert Morris' code stated that had Morris wanted to destroy vast reams of INTERNET data he need only have added a few lines of code to his worm--a task easily within the competence of Morris, a highly-regarded UNIX programmer.[33]

The "Michaelangelo" virus that destroys data on a PC hard disk can also destroy an SS7 database. ONA will require software "firewalls" to guard access. As outside access goes deeper into the core software network the risk of compromise will surely increase. The battle here is no different than the classic match-up of armor and shell, which began when Hector's spear pierced but 5 out of the 7 ox-hide folds of Ajax's shield. (The gods saved Hector that day; we may not have recourse to divine anti-viral intervention.)

C. Cyber-Law: Cyber-Crimes and Tele-Torts. The INTERNET disaster prompted a rash of stricter laws to punish abuse of computer networks. Morris himself received a suspended sentence--his act was, after all, not the culmination of a career of malicious hacking but rather a college kid's surrender to a spur-of-the-moment anti-social impulse, albeit causing huge financial harm.

As the network becomes more like a single, vast computer meta-network, the problems that plague the computer world are bound to intrude into the telecom world. *Wilkommen bienvenue, welcome*: viruses, Trojan horses, worms, bombs and whatever else might be conjured up on the Island of Dr. Moreau. The dark side of the Virtual Tele-World is here.

To "cyber-crimes" we must add "tele-torts." Those who use telephone networks to impair the reliability of the nationwide public network fabric must be held responsible. The FCC--and the states, for their part--should adopt "rules of the road" to minimize the danger of network software being manipulated by hostile users. Remember: *open access for the pharmacist is also open access for the drug dealer.*

What makes matters urgent, in this observer's view is that global software transparency *raises* the potential pay-off to software Darth Vaders--the damage from single-point failure is global. Nor can we count on user security alone: *just as a secret is as safe as the biggest gossip that knows it, a network is as secure as its most careless user.*

A 1989 report by the National Research Council assessed the FCC's ONA policy and recommended: "At minimum, the evolution of ONA should reflect security considerations as well as the desire to provide open, equal access for users.[34]

Open networks are a necessity if the benefits of the Information Age are to be realized. But no more than any of us would leave our front doors open should network providers be required to do so. *Open networks must become open secure networks.*

The equivalent of a "Software Part 68" is needed to address the range of technical and policy issues posed by potential abuse--accidental or intentional--of critical network software. At minimum, we need standards for testing, certification and registration of software, calibrated to authorization levels--with secure "firewalls" separating user- and system-level access. It will be necessary to coordinate any FCC action with ongoing activities of the NSTAC.

The NSTAC should continue its fine work in assessing software security threats and coordinating industry/government responses. The FCC should explore issues pertaining to legal responsibility and public policy: relative responsibility of vendors, service providers and common carriers; reconciling open access with network integrity and security; what knowledge, if any, a "reasonable user" should be deemed to have legal "notice" of; possible testing, certifcation and registration regulations. The two can go hand in hand: developing standardized tools such as audit trails can help fix responsibility for network harm.

Responsibility must follow control; where control lies, so lies responsibility. Those who link software to the core network should accept the same obligation imposed upon those connecting hardware: "First, do no harm." *Ease of access and ease of security are flip sides of the same coin; access without restriction is access without security.*

We are all familiar with three "famous last words": (1) "The check is in the mail"; (2) "Of *course* I'll respect you in the morning"; and (3) "Hi! I'm from the IRS and I'm here to help you."

In a software-driven world we can add a fourth to the list of classics: "Relax! This software is completely bug-free and absolutely secure."

We discount software risks at our peril.

[1] On July 9, 1990, three members of the Legion pled guilty to federal fraud charges in Georgia. *Telecommunications Reports*, July 16, 1990, p. 27. But the Legion's 911 caper ended in an anticlimax, as it turned out that the information necessary to access the 911 software, which a Legion member had broadcast over an electronic bulletin board, was also available from Bellcore via an 800-number, leading to some charges being dropped against members of the group. *Communications Daily*, July 31, 1990, pp. 2 - 3. The event did, however, show that 911 software was manipulated from outside. *Open Sesame: For Hackers Such as Frank Darden, There's Nothing More Inviting Than a Closed Door*, Wall Street Journal, August 22, 1990, p. 1.

[2] Vail: the architect of the modern Bell System; Armstrong: America's radio genius, inventing the super-heterodyne receiver and FM transmission, and recognized by his peers (but not the courts) as inventor of the triode vacuum tube; Shannon: the father of information theory; von Neumann: the father of the modern electronic digital computer; Noyce: co-inventor of the integrated circuit and founder of Intel Corporation. Bell? Your guess.

[3] The estimate comes from the Computer Virus Industry Association (San Jose, California). McAfee, John, *Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System*, p. 4 & p. 7 (St. Martin's Press, 1989).

[4] Hafner, Katie and Markoff, John, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, pp. 139 - 251 (Simon & Schuster, 1991).

[5] *Preliminary Report on Network Outages*, p. 8 (Common Carrier Bureau, July 1991). The report, albeit labeled "preliminary," was the only FCC document issued on the DSC STP crashes. It thus stands as the FCC's "final" statement on the matter.

[6] *Id.*, p. 5.. The SS 7 software vendor was DSC Communications Corporation.

[7] *Id.*, p. 1.

[8] *Id.*, p. 8.

[9] HR 4789, introduced by Rep. Edward J. Markey (D-7, MA) in the 102nd Congress. The bill did not reach mark-up stage. It has not been re-introduced, and no bill setting penalties is pending at this date.

[10] The NSTAC was formed in 1982, to address national security emergency preparedness (NS/EP) issues in light of the AT&T divestiture. NSTAC works closely with the National Communications System (NCS), established by President Kennedy in 1963 (after the Cuban Missile Crisis revealed a need for better crisis communications). NCS is part of the Defense Communications Agency. The NSTAC has considered software security issues, and continues to do so.

[11] Final Report of the Network Security Task Force (NSTAC, June 10, 1992). The task force is a sub-group established under the aegis of the NSTAC's Industry Executive Subcommittee (IES).

[12] *Id.*, p. 17. (Emphasis in original.)

[13] *Id.*, p. 18.

[14] *Id.*, p. 17.

[15] *Id.*, pp. 18 - 19.

[16] *Id.*, pp. 11 - 13.

[17] *AT&T v. Jiffy-Lube International, Inc.*, CIVIL NO. R-90-2400 (D.D.C., Md., filed February 18, 1993).

[18] Landreth, Bill, *Out of the Inner Circle*, pp. (Microsoft Press, 1989). A former hacker, Landreth disclosed techniques he used to gain "super-user" status. He was ultimately caught by the FBI and tried. After conviction, he was sentenced to community service and a small fine.

[19] Petition for Investigation, Coalition of Open Network Architecture Parties (filed November 16, 1990). CONAP's petition led to issuance of the FCC's Notice of Inquiry in CC Docket No. 91-346.

[20] *Id.*, p. 30.

[21] *Id.*, p. 32.

[22] *Id.*, pp. 7 - 8.

[23] According to one 1989 estimate, 70 percent of viruses struck IBM or IBM-compatibles, compared to 24 percent for Macintosh and Amiga systems, and 6 percent for all others. McAfee, note 3 *supra*, p. 60.

[24] *See generally*, Hoffman, Lance J. (Ed.), *Rogue Programs: Viruses, Worms and Trojan Horses* (Van Nostrand Reinhold, 1990).

[25] *Id.*, p. 300, quoting a consultant for Centel's FTS-2000 bid.

[26] *In the Matter of Intelligent Networks*, Notice of Inquiry, CC Docket No. 91-346 (released December 6, 1991).

[27] *Australia to Try Computer Hacker Accused of Damaging NASA Network*, Washington Post, August 15, 1991.

[28] Definitions: *Virus:* Program code embedded within a host program, which can only be activated by execution of the host and replicates itself into other hosts (*e.g.*, the Pakistani Brain, which infects floppy diskettes). *Worm:* An independent program that can execute and replicate itself, without prior execution of another program (*e.g.*, the Morris INTERNET worm, which clogged computer memory). *Trojan Horse:* A malicious program concealed within a legitimate program (*e.g.*, the "Sexy Ladies" program that erased sectors on Apple Macintosh hard disks while their users admired the screen display). *Time Bomb:* A program triggered by occurrence of a temporal event (*e.g.*, Michaelangelo, activated on March 6, the artist's birthday). *Logic Bomb:* A program triggered by occurrence of a logical condition (*e.g.*, certain key-strokes or commands; in 1988, an employee of a Fort Worth insurer/brokerage firm, Donald Gene Burleson, left a rogue program on the system of his former employer, USPA & IRA Company, which was triggered when his name was removed from the payroll list). Hoffman, note 24 *supra*, pp. 23 - 25 and p. 205.

[29] National Research Council, *Computers at Risk: Safe Computing in the Information Age* (National Academy Press, 1991), p. 7.

[30] *Phone Tie-Up Blocks Aid for Dying Woman*, Washington Times, July 24, 1992, p. C5.

[31] Some terrorists apparently do. The "PLO Virus" was implanted in computers at Israel's Hebrew University, to be activated on May 13, 1988, the 40th anniversary of the last full day of juridical existence for the League of Nations' 1920 Palestine Mandate (the day before official proclamation of the formation of the State of Israel). The virus replicated too quickly, and was discovered by Israeli technicians and neutralized before harm was done. *See* Fites, Philip, Johnston, Peter and Kratz, Martin, *The Computer Virus Crisis*, p. 30 (Van Nostrand Reinhold, 1989).

[32] *America's Hidden Vulnerabilities: Crisis Management in a Society of Networks*, A Report of the Joint Panel on Crisis Management of the CSIS Science and Technology Committee (1984). The Panel Co-Chairmen were R. James Woolsey, now CIA Director, and Robert H. Kupperman, a noted terrorism expert.

[33] Hoffman, note 24 *supra*, p. 221.

[34] National Research Council, *Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness* (National Academy Press, 1989), p. 37.