Hold the (Internet) Phone!
The Implications of Voice-over-Internet Protocol (VoIP) Telephony for National Security & Critical Infrastructure Protection

EMILY FRYE[*] & GREGORY STAITI[**]

ABSTRACT

As Voice over Internet Protocol (VoIP) is adopted as a means of voice communications over the next decade there may be serious national security consequences. At present, VoIP service providers have difficulty connecting users to local "9-1-1" call centers. In addition, law enforcement officials may not have the legal authority or technical capability to monitor criminal communications over VoIP. An even greater concern to public safety and national security exists in the very practice of sending voice and data over the same lines. The convergence of formerly independent communications networks exposes voice to vulnerabilities, such as Internet viruses and hacking, that were nonexistent on the public switched telephone network (PSTN). This risk is especially significant due to the heavy dependence of critical infrastructure sectors, such as the energy, financial services industries, and first responders, on reliable voice and data communications. VoIP is replete with promise, but security issues must be addressed or its economic benefits could be lost in the wake of a malicious attack.

I. INTRODUCTION

After years of relative obscurity, Voice-over-Internet Protocol (VoIP) telephony appears ready to go mainstream. VoIP is likely to become the primary means of voice communications within the next decade, given its considerable economic advantages over traditional

[*] Emily Frye is Associate Director for Law and Economics at the Critical Infrastructure Protection Program of George Mason University School of Law. She directs interdisciplinary research focused on the law and policy surrounding homeland security.

[**] Gregory Staiti is a *Juris Doctor* candidate, May 2006, at George Mason University School of Law. He served as legal intern to the Critical Infrastructure Protection Program during Summer 2004.

telecommunications services. Individual consumers see VoIP as an opportunity to lower their monthly bills, because VoIP is currently free from government regulations that otherwise raise service fees for customers. Businesses reap the cost savings, too. They are also attracted by VoIP's current and next-generation functional abilities, such as integrated voice and email messaging and people-finder capabilities, which can increase operational efficiency. For communications service providers, VoIP is a way to get more "bang for their buck" by leveraging existing wireline networks to pull double-duty for voice and data communications. The federal government views VoIP as a boon to achieving nationwide broadband deployment goals.

Largely unnoticed in the rush to VoIP adoption is the fact that unmoderated embrace of VoIP has serious national security consequences. With current technology, VoIP service providers have difficulty connecting users to local "9-1-1" call centers, and almost certainly cannot guarantee that the receiving center will match the user's location. In addition, law enforcement officials may not have the legal authority or technical capability to monitor criminal communications over VoIP. These problems, like others concerning universal service and interconnection requirements in the telecommunications arena, have been the subject of substantial public debate by federal regulators and lawmakers.

An even greater concern to public safety and national security, and one which has received less public attention, exists in the very practice of sending voice and data over the same lines. The convergence of formerly independent communications networks exposes voice to vulnerabilities, such as Internet viruses and hacking, that were nonexistent on the public switched telephone network (PSTN). This risk is especially significant due to the heavy dependence of critical infrastructure sectors, such as the energy, financial services industries, and first responders, on reliable voice and data communications. VoIP is replete with promise, but security issues must be addressed or its economic benefits could be lost in the wake of a malicious attack.

II. VoIP Technology: Current and Future Prospects

A. An Overview of VoIP Technology

VoIP services work much like traditional data transmission: voice sounds are broken down into binary code, distributed across data networks, and reassembled at the receiver's location.[1] This process differs from traditional communications over the PSTN, which requires a single dedicated logical connection between beginning and end users for the duration of the call.[2] The practice of sending voice as data over the Internet "is a relatively old concept, in Internet years."[3] Only recently, however, have improvements in the underlying technology brought VoIP to the level of maturity that makes widespread consumer adoption possible.[4] As a result, the public network (PN), which formerly consisted of logically separate communications and data networks, sharing only common transmission facilities, now "increasingly consists of converged networks ... [with] circuit switched networks interoperating with broadband packet-based Internet Protocol (IP) networks."[5]

The mode of connecting users and the degree of interconnection with the PSTN differs between VoIP service providers. As Federal Communications Commission (FCC or the Commission) Chairman Michael Powell observed in February 2004:

> Some of these Internet voice services will be delivered over the public Internet; others will use Internet protocols over private networks to reach end-users. Some of these services will be Internet-only applications; others will allow Internet

[1] *See* FCC.COM, Voice Over Internet Protocol Frequently Asked Questions, *at* http://www.fcc.gov/voip (last accessed May 24, 2004) ("VoIP converts the voice signal from your telephone into a digital signal that travels over the internet then converts it back at the other end ....").

[2] *Cf.* Nicholas Thompson, *Sir, to Whom May I Direct Your Free Call?*, N.Y. TIMES, Oct. 12, 2003, at §3, p.1 ("In the regular phone network, calls initially pass over less efficient copper wires and the phone companies must maintain dedicated connections between users ....").

[3] Lisa Guernsey, *The Web Discovers Its Voice*, N.Y. TIMES, Oct. 21, 1999, at G8 (noting that "Internet telephony companies have been converting sound into data packets since the mid 1990's ....").

[4] *See* Barnaby J. Feder, *Judge Says Minnesota Cannot Regulate Internet Calls*, N.Y. TIMES, Oct. 9, 2003, at C8 ("The new voice technology is being driven by improvements in microelectronics that allow Internet networks to break voice traffic up into digital data packets and deliver it around the globe without the interruptions and sacrifices in voice quality that hampered early versions.").

[5] THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE, CONVERGENCE TASK FORCE REPORT (2001), *available at* http://www.ncs.gov/nstac/reports/2001/ConvergenceReport-Final.htm (last accessed July 8, 2004) [hereinafter NSTAC CTF REPORT].

> callers to reach out to users on the public switched telecommunications network. Some will be pay services; others will be free or simple add-ons to other types of applications. All, however, will enhance our ability to communicate with each other.[6]

B. FACTORS DRIVING VOIP ADOPTION

In addition to improvements in quality of service, other factors have played a significant role in driving the recent push toward widespread VoIP adoption. One factor, which is perhaps too often credited, is the lack of regulatory oversight of VoIP service providers. The FCC is currently considering whether VoIP service providers should be subject to traditional telecommunication requirements, but has not yet regulated providers as it regulates traditional telecommunications.[7] Similarly, although Minnesota[8] and New York[9]

[6] *Hearing on Voice over Internet Protocol (VOIP) Before the Senate Comm. on Commerce, Science & Transp.*, 108th Cong. 4 (2004) (statement of Michael K. Powell, Chairman, Fed. Communications Comm'n), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-244231A1.pdf (last accessed Aug. 13, 2004) [hereinafter Powell Statement].

[7] *See generally* FED. COMMUNICATIONS COMM'N, IN THE MATTER OF IP-ENABLED SERVICES NOTICE OF PROPOSED RULEMAKING (2004), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-28A1.pdf (last accessed Sept. 17, 2004) [hereinafter IP-ENABLED SERVS. NPRM]. To date, the FCC has issued only two decisions concerning the applicability of economic regulations to VoIP. In February 2004, concurrent with the issuance of the broader NPRM cited above, the FCC examined pulver.com's "Free World Dialup" (FWD), a limited VoIP service that provides "free communications over the Internet between one on-line FWD member using a broadband connection and other on-line FWD members using a broadband connection." FED. COMMUNICATIONS COMM'N, IN THE MATTER OF PETITION FOR DECLARATORY RULING THAT PULVER.COM'S FREE WORLD DIALUP IS NEITHER TELECOMMUNICATIONS NOR A TELECOMMUNICATIONS SERVICE 2 n.3 (2004), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-27A1.pdf (last accessed Sept. 17, 2004) [hereinafter FWD DECLARATORY RULING]. The Commission determined that the service provided by FWD was neither "telecommunications" nor "telecommunications service" and thus not subject to FCC regulatory requirements. *See id.* at 6-7. In April 2004, the Commission considered a substantially different application of VoIP technology by AT&T. AT&T petitioned the Commission to exempt its practice of converting calls initiated on the PSTN to IP format for transport over AT&T's Internet backbone before reconstituting the data on the PSTN again for the end-user. *See* FED. COMMUNICATIONS COMM'N, IN THE MATTER OF PETITION FOR DECLARATORY RULING THAT AT&T'S PHONE-TO-PHONE IP TELEPHONY SERVICES ARE EXEMPT FROM ACCESS CHARGES 1 (2004), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-97A1.pdf (last accessed Sept. 17, 2004). The FCC denied the petition, determining that AT&T's specific process is a telecommunications service covered by Commission regulations. *See id.* at 9.

have attempted to introduce performance requirements for VoIP providers, most states have not yet addressed whether their own regulatory programs should be extended to VoIP. In fact, the FCC is likely to contest those that attempt to do so.[10] This regulatory void has created an arbitrage opportunity in which VoIP service providers can provide nearly the same product as traditional telecommunications companies at reduced cost, producing savings that can be passed on to customers.[11] In addition, the lack of regulatory costs creates lower entry fees for startup VoIP providers, with the resulting competition further driving down consumer prices.[12]

[8] In September 2003, the Minnesota Public Utilities Commission (MNPUC) ordered Vonage, a VoIP service provider, to comply with Minnesota's statutes and regulations concerning the offering of telephone service. Vonage Holdings Corp. v. Minn. Pub. Utilities Comm'n, 290 F. Supp. 2d 993, 996 (D. Minn. 2003). The United States District Court for the District of Minnesota subsequently enjoined the MNPUC from regulating Vonage's VoIP services, concluding that "[s]tate regulation would effectively decimate Congress's mandate that the Internet remain unfettered by regulation." *Id.* at 994.

[9] *See, e.g.*, Press Release, N.Y. Pub. Serv. Comm'n, PSC: Vonage is a Telephone Corporation as Defined by NYS Law 2 (May 19, 2004), *available at* http://www3.dps.state.ny.us/pscweb/WebFileRoom.nsf/ArticlesByCategory/06086843A52CFBF085256E990060FC3B/$File/pr04038.pdf?OpenElement (last accessed Aug. 13, 2004). The New York Public Service Commission determined that Vonage, a VoIP service provider, "owns and manages equipment that is used to provide telephone service to Vonage's customers and to connect Vonage's customers to the customers of other telephone corporations via their public networks and thus, like other owners of telecommunications-provisioning equipment, is subject to the NYS Public Service Law." *Id.*

[10] *See* Griff Witte, *Few Rules Better for Calls on Internet, Powell Says*, WASH. POST, Feb. 25, 2004, at E2 ("Although some states have initiated regulations, the FCC has shown signs of late that it intends to take the lead in determining how VoIP is handled ...."). *See also* Ellen Muraskin, *FCC's Powell Reassures VOIP Community*, EWEEK.COM, June 23, 2004 (discussing FCC Chairman Michael Powell's position "'that those individual states that have taken an aggressive posture on regulating VOIP as a telecom service are making a mistake, since IP networks, like the railroads, are national and even global entities'"), *at* http://www.eweek.com/article2/0%2C1759%2C1616394%2C00.asp (last accessed Apr. 22, 2005).

[11] *See* Chérie R. Kiser & Angela F. Collins, *Regulation on the Horizon: Are Regulators Poised to Address the Status of IP Telephony?*, 11 COMMLAW CONSPECTUS 19 (2003).

[12] Powell Statement, *supra* note 6, at 6 ("[H]ungry, free radical entrepreneurs and software developers are taking advantage of extremely low entry barriers to pour investments into service offerings .... Lower entry and transaction costs are allowing Internet voice services to be offered at low prices, in some instances, for free.").

Beyond regulatory freedom, VoIP's enhanced communications features are also fueling its adoption.[13] Current VoIP services offer "multimedia and unified messaging capabilities ... [that] are not available over traditional local and long-distance service."[14] Meanwhile, next generation VoIP networks will leverage "the ubiquity of IP as a networking technology ... [to deploy] a vast range of innovative converged voice and data services that simply cannot be cost effectively supported over today's PSTN infrastructure."[15]

Operational efficiency is also a significant driver for VoIP adoption. For communications providers, the business rationale is simple:[16] VoIP "leverages data network capacity[,] removing the requirement to operate separate voice and data networks."[17]

[13] *Hearing on Voice over Internet Protocol (VOIP) Before the Senate Comm. on Commerce, Science & Transp.*, 108th Cong. (2004) (statement of Kevin Werbach, Founder, Supernova Group LLC) (explaining that VoIP has grown not due to regulatory arbitrage, but "because it's a better technology ... [that] is more efficient, and more flexible, than the legacy circuit-switched technology"), *available at* http://commerce.senate.gov/hearings/ testimony.cfm?id=1065&wit_id=2993 (last accessed Aug. 13, 2004) [hereinafter Werbach Statement].

[14] Lisa Pierce, *Commentary: Heads Up VoIP – Regulation Incoming*, CNET NEWS.COM, Apr. 8, 2004, *at* http://news.com.com/2030-7352-5188097.html (last accessed June 10, 2004). For example, Vonage customers can utilize web based voicemail retrieval and online features management. *Hearing on Voice over Internet Protocol (VOIP) Before the Senate Comm. on Commerce, Science & Transp.*, 108th Cong. 3 (2004) (statement of Jeffrey Citron, Chairman and Chief Executive Officer, Vonage Holdings Corp.), *available at* http://commerce.senate.gov/pdf/citron022404.pdf (last accessed Aug. 13, 2004).

[15] MULTISERVICE SWITCHING FORUM, MSF TECHNICAL REPORT: NEXT-GENERATION VOIP NETWORK ARCHITECTURE 5 (2003), *available at* http://www.msforum.org/techinfo/reports/ MSF-TR-ARCH-001-FINAL.pdf (last accessed July 8, 2004) [hereinafter MSF TECHNICAL REPORT]. (According to their website, "[t]he MultiService Forum (MSF) is a global association of service providers and system suppliers committed to developing and promoting open-architecture, multiservice switching systems ... MSF's activities include developing implementation agreements, promoting worldwide compatibility and interoperability, and encouraging input to appropriate national and international standards bodies." MultiService Forum, About MSF: Who We Are, *at* http://www.msforum.org/about/who.shtml (last accessed Sept. 17, 2004)).

[16] *See* Michael A. Hiltzik, *A New Calling for the Net*, LOS ANGELES TIMES, May 29, 2000, at A1 (quoting Noam Bardin, chief executive of DeltaThree, a telecommunications company: "'Today [there are] two networks .... One does everything, and the other does only voice. That means the phone network has no real technological reason to be around in the future.'").

[17] MSF TECHNICAL REPORT, *supra* note 15, at 5.

Furthermore, equipment used to run VoIP is often faster and cheaper than traditional telephony equipment.[18]

Given the quality of service and economic rationales driving end-user adoption, more and more companies are beginning to offer VoIP. Startup VoIP providers are experiencing rapid growth,[19] and the major telephone,[20] cable,[21] and even computer technology[22] firms are establishing the technological foundations for future nationwide service. VoIP may prove to be the "killer app" that drives broadband access and enrollment across the United States.[23] Yet VoIP is not without its drawbacks, some of which have been the subject of intense debate among federal regulators and lawmakers.

III. CURRENTLY-IDENTIFIED VOIP PUBLIC SAFETY ISSUES

In February 2004, FCC Chairman Michael Powell identified several key public safety issues surrounding VoIP in which federal

[18] *Id.*

[19] For example, in February 2004, Vonage activated its 100,000th line, just 5 months after having activated its 50,000th line. *Hearing on Voice over Internet Protocol (VOIP) Before the Senate Comm. on Commerce, Science & Transp.*, 108th Cong. 1 (2004) (statement of Jeffrey Citron, Chairman and Chief Executive Officer, Vonage Holdings Corp.), *available at* http://commerce.senate.gov/pdf/citron022404.pdf (last accessed Aug. 13, 2004) [hereinafter Citron Statement].

[20] *See, e.g.*, Press Release, AT&T, Dorman Outlines Aggressive, Continuing transformation of AT&T as the "World's Networking Company" (Feb. 25, 2004) (discussing AT&T's plans to provide VoIP in one hundred markets nationwide by the end of 2004), *at* http://www.att.com/news/2004/02/25-12936.

[21] *See, e.g.*, *Hearing on Voice over Internet Protocol (VOIP) Before the Senate Comm. on Commerce, Science & Transp.*, 108th Cong. (2004) (statement of Glenn Britt, Chairman and Chief Executive Officer, Time Warner Cable) (discussing his company's plans to provide VoIP service "throughout the majority of the Time Warner Cable footprint by the end of 2004"), *available at* http://commerce.senate.gov/hearings/testimony.cfm?id=1065&wit_id=2990 (last accessed Aug. 13, 2004) [hereinafter Britt Statement].

[22] *See, e.g.*, Keith Regan, *IBM, Cisco Ally for VoIP Push*, TECHNEWSWORLD.COM, May 18, 2004 (discussing a partnership between IBM and Cisco Systems to work together on future VoIP projects), *at* http://www.technewsworld.com/story/33848.html (last accessed May 21, 2004).

[23] *See* Powell Statement, *supra* note 6, at 2 ("Just as email and e-commerce were drivers of the narrowband Internet, higher bandwidth applications like ... Internet voice will be the 'killer apps' for broadband.").

government action may be necessary, including 9-1-1 and law enforcement access.[24] Although not the focus of this paper, these issues are briefly summarized below.

A. "9-1-1" / "E9-1-1" CAPABILITIES

Two primary concerns have been identified regarding VoIP's "9-1-1" and "E9-1-1" capabilities: (1) callers may not be able to connect to 9-1-1 dispatch centers; and (2) there is no guarantee that callers' location information is correct when sent to a 9-1-1 dispatch center from a VoIP system.[25]

In order for VoIP service providers to connect to dedicated lines on the PSTN for a Public Safety Answering Point (PSAP), they must obtain interconnection with incumbent local exchange carriers (LECs).[26] Some LECs have refused to cooperate with VoIP services in providing 9-1-1 access.[27] Confusion about source locations results from the portability of VoIP services: "[m]ost IP telephones can be easily moved from one LAN port to another without reprogramming ... [which] can cause problems if the physical location of the telephone is different from the location reported to emergency personnel."[28]

A variety of solutions have emerged to address this problem. As an interim fix, some VoIP providers include an express disclaimer about their 9-1-1 connection limitations.[29] Others suggest maintaining emergency telephones connected to the PSAP through traditional telephone lines at various points in the caller's building.[30] The FCC

[24] Powell Statement, *supra* note 6, at 9.

[25] *See supra* note 1 ("It may be difficult for some Internet Voice services to seamlessly connect [sic] with the 911 dispatch center or identify the location of Internet Voice 911 callers.").

[26] Citron Statement, *supra* note 19, at 8.

[27] *See id.*

[28] HEWLETT PACKARD, TECHNICAL BRIEF: NETWORK INFRASTRUCTURE: GETTING STARTED WITH VoIP 5 (2003), *available at* http://h41111.www4.hp.com/procurve/uk/en/pdfs/final_voip_techbrief.pdf (last accessed April 4, 2005) [hereinafter HP TECHNICAL BRIEF].

[29] *See, e.g.*, Citron Statement, *supra* note 19, at 9 ("Vonage makes the limitations inherent in its 911 service clear to all Vonage customers.").

[30] *See* HP TECHNICAL BRIEF, *supra* note 28, at 5.

and States such as Minnesota are considering government action to ensure 9-1-1/E9-1-1 availability for VoIP users.[31] VoIP service providers recognize that their technology might ultimately produce better 9-1-1 service than current offerings on the PSTN, and that this functionality might prove a selling point.[32] Thus, VoIP providers have incentives beyond regulatory requirement to invest in future 9-1-1 and E9-1-1 capabilities.[33]

B. LAW ENFORCEMENT ACCESS TO VOIP CONVERSATIONS

Another hotly contested issue in recent months has been the debate surrounding whether VoIP service providers must comply with the

[31] IP-ENABLED SERVS. NPRM, *supra* note 7, at 38 ("Assuming that [the FCC] find[s that] IP-enabled services in general or certain services in particular to [sic] fall within [its] E911 'scope' criteria, [the FCC] seek[s] comment on how best to achieve [its] policy objectives for ensuring the availability of 911 and E911 capability."). The E911 Scope Criteria used by the FCC to determine whether communications providers should be subject to 911/E911 regulation include:

> (1) the entity offers real-time, two-way switched voice service, interconnected with the [PSTN] ...;
>
> (2) customers using the service or device have a reasonable expectation of access to 911 and enhanced 911 services; (3) the service competes with traditional CMRS or wireline local exchange service; and (4) it is technically and operationally feasible for the service or device to support E911.

Id.

[32] *See* Citron Statement, *supra* note 19, at 8 ("[U]ltimately VoIP will offer consumers and emergency workers more functionality than the services of today. For example ... emergency workers may be able to instantly and seamlessly access that customer's medical history, while at the same time a separate message could notify the customer's primary physician or family members of the emergency situation.").

[33] Ongoing technological developments can certainly address the quality of 9-1-1 offerings, provided the market adopts them. For instance, current efforts under way at the National Emergency Number Association and at the Internet Engineering Task Force are developing standards for providing location information in conjunction with an IP address. Separately, telecommunications giant Verizon recently announced that it would "provide Voice-over-Internet-Protocol (VoIP) service providers and their vendors the ability to use Verizon's Enhanced 911 emergency calling system to connect VoIP customer 911 calls to Public Safety Answering Points (PSAPs)." Press Release, Verizon, Verizon Identifies Solution Enabling VoIP Companies to Connect to E 911 Emergency Calling System (Apr. 26, 2005), *available at* http://newscenter.verizon.com/proactive/newsroom/release.vtml?id=90778 (last accessed May 12, 2005). These efforts, among a host of others, indicate that VoIP providers are acutely aware of the need to offer 9-1-1 and E-9-1-1 capabilities.

Communications Assistance for Law Enforcement Act (CALEA).[34] CALEA establishes requirements for telecommunications carriers to intercept customers' communications, and to provide law enforcement access to the intercepted communications pursuant to a court order or other lawful authorization.[35] VoIP services pose two problems for CALEA compliance. After prolonged uncertainty,[36] the Federal Communications Commission has recently ruled that VoIP should, in fact, be classified as a "telecommunications service"[37] rather than an "information service"[38] as defined by the Telecommunications Act. Therefore, the Telecommunications Act covers VoIP and requires that VoIP providers support CALEA. This resolution, however, comes after VoIP protocols have already been in place in a non-compliant mode, leading to a second, and perhaps more significant, compliance

[34] For example, in his statement concerning the FCC's decision that "pulver.com" was an unregulated information source, Commissioner Michael J. Copps stated that he "would dissent to this item purely on law enforcement and national security grounds. The Communications Assistance for Law Enforcement Act (CALEA) expressly exempts entities providing information services from complying with law assistance capability requirements. No assurances from companies ... have yet demonstrated a satisfactory solution to this thorny problem." FWD DECLARATORY RULING, *supra* note 7, at 24.

[35] *See* 47 U.S.C. § 1002(a) (2000).

[36] *Compare* ELECTRONIC PRIVACY INFORMATION CENTER, COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER IN THE MATTER OF COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT JOINT PETITION FOR RULEMAKING 3 (2004) ("[t]he language of CALEA ... unambiguously excludes information services such as e-mail and Internet access"), *available at* http://www.epic.org/privacy/wiretap/calea/caleacomment4.12.04.pdf (last accessed Aug. 13, 2004) [hereinafter EPIC COMMENTS] *with* Kiser & Collins, *supra* note 11, at 32 ("A finding that IP telephony is an information service ... would not necessarily relieve providers from complying with CALEA .... [T]he [FCC] has authority under CALEA to reach any provider of 'wire or electronic communication switching or transmission service to the extent that ... such service is a replacement for a substantial portion of the local telephone exchange service.'").

[37] "Telecommunications service" is defined as "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used." 47 U.S.C. § 153(46) (2000). "Telecommunications" is defined as "the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received." 47 U.S.C. §153(43) (2000).

[38] "Information service" is defined as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service." 47 U.S.C. §153(20) (2000).

challenge: the *ability* of VoIP service providers to comply with CALEA requests is uncertain. VoIP decouples the voice application from the underlying transmission facilities; "the provider that interfaces with the end-user may only have access to call *routing* information" and would be unable to comply with law enforcement requests for call *content*.[39] And due to the packetized nature of VoIP data transmission, when call content *is* available to law enforcement, the voice data packets sought by law enforcement may be jumbled with innocent third party content, raising privacy concerns.[40]

Ultimately, some form of VoIP compliance with CALEA will likely be required. Law enforcement[41] and business leaders[42] are (understandably) concerned that VoIP not become a "safe haven" for criminal and terrorist communications, beyond the purview of lawful surveillance. Federal regulators[43] and lawmakers[44] currently are

[39] *See* Werbach Statement, *supra* note 13.

[40] EPIC COMMENTS, *supra* note 36, at 6 ("[S]urveillance conducted in packet-mode environments can result – and indeed *has* resulted – in the unauthorized capture of third-party communications.").

[41] In a June 2004 hearing on VoIP legislation, Deputy Assistant Attorney General Laura Parsky expressed the U.S. Department of Justice's concern that "when it becomes known that law enforcement has difficulty detecting communications over a particular technology, criminals quickly migrate to that technology. *Hearing on The VOIP Regulatory Freedom Act, S. 2281, Before the Senate Comm. on Commerce, Science and Transp.*, 108th Cong. (2004) (statement of Laura Parsky, Deputy Assistant Attorney General, Criminal Division, U.S. Dep't of Justice), *available at* http://commerce.senate.gov/hearings/ testimony.cfm?id=1230&wit_id=3537 (last accessed July 8, 2004) [hereinafter Parsky Statement].

[42] An anonymous senior source in the financial community has indicated to the CIP Program that terrorists and criminal conspiracies are transferring the bulk of their voice communications to Internet channels because service providers are not currently required to comply with CALEA.

[43] In August 2004, the FCC issued a notice of proposed rulemaking that "tentatively conclude[d]," among other things, that "'managed' Voice over Internet Protocol ('VoIP') services are subject to CALEA." FED. COMMUNICATIONS COMM'N, IN THE MATTER OF COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT AND BROADBAND ACCESS AND SERVICES 2 (2004), *available at* http://www.askcalea.net/docs/20040809.fcc.04-187.pdf (last accessed Sept. 17, 2004). "Managed" VoIP includes those services whereby the VoIP provider "manage[s] the communication between its end points and ... provide[s] call set up, connection, termination, and party identification features ...." *Id.* at 19.

[44] *See, e.g.*, S. 2281, 108th Cong. § 4(c) (2004); H.R. 4129, 108th Cong. § 4(c) (2004). Although §4(c) was removed as the bill was reported out of committee, the inclusion of the original language indicates a growing awareness and concern in the legislative branch about limitations on law enforcement functionality in an age of rapid technical change.

attempting to address the appropriate means of ensuring law enforcement access to VoIP communications.

IV. THE NATIONAL SECURITY / CRITICAL INFRASTRUCTURE CONCERN WITH VOIP

The public safety issues discussed in the preceding section are important and merit public attention. An even more far-reaching concern, however – the security implications of converged voice and data networks – has received considerably less attention from regulators and lawmakers.[45]

A. VOIP INTRODUCES VULNERABILITIES TO VOICE COMMUNICATION

The reliability of communications over the PSTN has come to be taken for granted by Americans. Business and government operate, and are built upon, an assumption of ubiquitous telephone service.[46] VoIP could change both the perception and the reality of ever-present telephone service because it suffers the same vulnerabilities to malicious electronic attack as other digital networking technologies.[47] VoIP also provides malicious agents with simpler means of reaching previously inaccessible targets.[48] Four particular vulnerabilities could

[45] As the reader will notice from the citations that follow, this paper does not imply that VoIP security has received no attention at any level of government. In particular, the President's National Security Telecommunications Advisory Committee (NSTAC) has authored several relevant task force reports over the last three years on the issue of convergence; however, these reports discuss convergence issues in the context of an interim period of interoperation between the PSTN and IP voice networks before full transition to the next generation "all-IP" network. This paper is distinguished from the NSTAC reports because it focuses on vulnerabilities of converged voice and data on the same digital backbone – i.e., what the NSTAC reports refer to as the next generation network (NGN). Nonetheless, many of the convergence vulnerabilities identified by the NSTAC must also be addressed in the NGN.

[46] Hiltzik, *supra* note 16 (discussing the 99.999%, or "five nines" expected uptime for PSTN communications).

[47] *See* Jim Louderback, *Security Holes Make VOIP a Risky Business*, EWEEK.COM, May 12, 2004, *at* http://www.eweek.com/article2/0,1759,1591127,00.asp (last accessed Apr. 4, 2005); *see also* Matthew Broersma, *VOIP's Cry: More Secure Data Nets*, EWEEK.COM, June 10, 2004, ("[V]oice running on a company's IP network is just like any other application, with the same kinds of vulnerabilities and similar processes for ensuring security"), *at* http://www.eweek.com/article2/0,1759,1609840,00.asp (last accessed Apr. 4, 2005).

[48] *See, e.g.*, NSTAC CTF REPORT, *supra* note 5 (discussing concerns that the interoperation of the PSTN and IP networks could provide "a 'back door' into the control space of the PSTN, which could enable malicious activities such as insertion of false [signaling] messages").

prove especially problematic for national and economic security: (1) susceptibility to a "denial of service" attack; (2) identity spoofing; (3) power dependence; and, (4) cascading disruptions due to interconnection of networked systems.

1. DENIAL OF SERVICE IN THE VOICE REALM

Denial of Service (DoS) attacks have become all-too-familiar in Internet computing.[49] A DoS attack basically involves "flood[ing] a server with packets in an attempt to disrupt service."[50] DoS-type attacks are possible in the PSTN – for example, a malicious actor can set an autodialer to redial a number repeatedly, thus mimicking the information overload aspect of an IP-based DoS attack.[51] By putting voice on IP networks, however, VoIP expands the scale of such attacks while lowering the cost to do so. Rather than targeting one user with an autodialer, a malicious agent can disrupt *all* users' ability to make a VoIP phone call by attacking their service provider's servers.[52] Furthermore, with the increased availability of "user-friendly tools" to conduct DoS attacks, even "less knowledgeable hackers [can] conduct attacks with relative ease."[53]

The network congestion caused by DoS attacks over networks used by VoIP applications could collaterally, if not directly, impact critical

[49] Perhaps the most infamous of these attacks were the "Code Red" worms of 2001, which exploited a vulnerability in Microsoft Internet Information Server (IIS) Web server software to install themselves on multiple computer systems, which then participated in a sophisticated "distributed denial of service" (DDoS) attack on the White House website. The Code Red worms "illustrated how widespread automated propagation of malicious code has developed into a means for establishing the foundation for DDoS attacks." THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE, NETWORK SECURITY/ VULNERABILITY ASSESSMENTS TASK FORCE REPORT (2002), *available at* http://www.ncs.gov/ nstac/reports/2002/NSVATF-Report-(FINAL).htm (last accessed Aug. 5, 2004) [hereinafter NSTAC VATF REPORT].

[50] Ellen Muraskin, *A Pioneer's View of VOIP and SIP Security*, EWEEK.COM, May 17, 2004, *at* http://www.eweek.com/article2/0,1759,1593991,00.asp (last accessed April 4, 2005).

[51] *See* Roger W. Farnsworth, *Enterprise Security - an Enabler of VoIP*, CONVERGE NETWORK DIGEST, July 6, 2004, *at* http://www.convergedigest.com/blueprint/ttp04/ z4cisco2.asp?ID=141&ctgy=4 (last accessed July 8, 2004).

[52] *See* NSTAC CTF REPORT, *supra* note 5 ("[A] denial of service (DOS) attack on a particular ISP could impede data traffic flows, Web site accessibility, and VoIP service availability and reliability.").

[53] NSTAC VATF REPORT, *supra* note 49.

national security/emergency preparedness (NS/EP) communications.[54] For example, emergency telecommunications access programs, such as the Government Emergency Telecommunications Service (GETS), may not work properly (as currently conceived) in an all-IP voice communications network.[55] These programs function by according higher priority to participants' emergency communications during periods of congestion on the PSTN.[56] Priority is determined by signaling information, which – significantly – "provides call setup and call services *separate* from the actual transport of the voice data" on the PSTN.[57] As the NSTAC observed, VoIP communications – over IP networks – differ as follows:

> [I]n IP networks, the network intelligence data is transmitted over the same infrastructure as the data itself. Therefore, in IP-based networks, signaling messages are not accorded any higher priority than any other data or voice traffic in the network. During periods of congestion, signaling messages are as likely to be blocked or dropped as any other messages. In a converged network, such events could impact availability and reliability of the GETS service, which relies on the signaling network for functionality.[58]

Such collateral impacts would not only disrupt critical communications, but might also *instigate* an emergency event.[59]

[54] *See id.* ("As attack techniques increase in sophistication and intruders continue using DDoS techniques to exploit vulnerabilities, cyber attacks will likely cause greater collateral damage.").

[55] NSTAC CTF REPORT, *supra* note 5.

[56] *See* National Communications System, GETS Program Information, *at* http://gets.ncs.gov/program_info.html (last accessed Sept. 17, 2004).

[57] NSTAC CTF REPORT, *supra* note 5 (emphasis added).

[58] *Id.* Note that the report's conclusion recommends various mitigation tactics. The feasibility and horizon of these tactics needs to be explored further.

[59] NETWORK RELIABILITY AND INTEROPERABILITY COUNCIL VI, HOMELAND SECURITY – PHYSICAL SECURITY (FOCUS GROUP 1A) FINAL REPORT 50 (2003) ("[A]ttacks against network software could disrupt or otherwise compromise critical communications or operations during an emergency situation, or could in themselves precipitate an emergency situation."), *available at* http://www.nric.org/fg/charter_vi/fg1/ Rauscher_NRIC_VI_Homeland_Security_Physical_Security_Focus_Group_1A_Final_Report

2. IDENTITY SPOOFING

VoIP also presents hackers with increased opportunity to misrepresent their identity to spoof caller ID mechanisms.[60] While caller ID spoofing is possible on the PSTN, it comes "with a high price tag: you typically [have] to be a business able to pay the local phone company for a high-volume digital connection."[61] VoIP lowers the cost of misrepresentation because spoofing capabilities are in the possession of "ordinary netizens," rather than a large, heavily regulated industry.[62]

ID spoofing can be innocent but aggravating – for example, a VoIP user with caller ID might be tricked into answering the phone on a "VoIP Spam" call.[63] But spoofing can also pose a serious threat to business (and therefore economic security). For example, hackers could attempt to capture confidential business information by spoofing caller ID in a "phishing-style attack" and masquerading as an innocent vendor or sales group.[64] Alternatively, a VoIP user could misrepresent his identity to slip past authentication safeguards used by certain industries to prevent access to critical information or utilities.[65]

_Issue_3.doc (last accessed Apr. 4, 2005) [hereinafter NRIC PHYSICAL SECURITY FINAL REPORT].

[60] Kevin Poulsen, *VoIP Hackers Gut Caller ID,* THE REGISTER, July 7, 2004, *at* http://www.theregister.co.uk/2004/07/07/hackers_gut_voip/ (last accessed July 8, 2004).

[61] *Id.*

[62] *Id.*

[63] *Cf.* Muraskin, *supra* note 50 ("Spam ... is hard to stop ... unless [a VoIP user] fundamentally limit[s] who can call [her] (which is the approach in closed networks).").

[64] *See* Louderback, *supra* note 47.

[65] *See* NSTAC CTF REPORT, *supra* note 5 ("[B]y spoofing address sources, unauthorized individuals could access secure components of the PSTN via gateways."). *See also* Poulsen, *supra* note 60 (noting that some financial institutions use Caller ID to authenticate customers over the phone). One logical approach to preventing unauthorized access entails increasing the level and reliability of authentication used to verify the identities and entitlements of network participants. An experiment in the effectiveness of this approach can be seen in the AmericaOnline Instant Messenger enhancements, which do not permit interconnection with other instant messaging services using lower levels of authentication. From an end user perspective, this can be very frustrating. Teenagers – the true experts in emerging technology – perform end runs around this problem by using non-AOL instant messaging services, thereby pointing out the weakness in the approach.

3. ELECTRICITY DEPENDENCE

Electric power is frequently overlooked by businesses and consumers as a critical element of telecommunications.[66] This may be due, in part, to the fact that the electricity that travels over PSTN lines allows conventional (i.e., non-cordless) telephones to continue operating even during a power outage.[67] In contrast, VoIP telephones require an external power source, and as such are not as resilient during a power outage.[68] Consequently, VoIP communications during a power outage are impacted just as data transmission is impacted. The loss of phone communications during a power outage could seriously disrupt businesses' recovery plans.[69]

To provide communications during a power outage, VoIP network infrastructure must be connected to uninterruptible power supplies (UPS).[70] Unfortunately, VoIP service providers may not offer backup power.[71] Furthermore, backup power sources are not infallible,[72] and are often not designed for extended use.[73] Not only must the

[66] *See* NRIC PHYSICAL SECURITY FINAL REPORT, *supra* note 59, at 44.

[67] Kiser & Collins, *supra* note 11, at 41.

[68] *See id.* ("Because packet-switched networks do not have the same built-in power source that circuit-switched networks do, they are far more likely to be subject to service outages."). A new generation of technology is becoming available to address this problem, but the technology is not widely adopted. It includes DSL modems that are line powered, and ISDN NT1 equipment which provides emergency power from the central operating center to power digital ISDN handsets.

[69] *Cf.* PACIFIC NORTHWEST ECONOMIC REGION, "BLUE CASCADES" FINAL REPORT 3, 4 (2002) (discussing participants' lack of contingency plans for the loss of both telephonic and internet communication during a simulated power disruption of the Pacific Northwest region's electric power capabilities), *available at* http://www.naruc.org/associations/1773/files/bluecascades.pdf (last accessed June 24, 2004).

[70] HP TECHNICAL BRIEF, *supra* note 28, at 5.

[71] FCC.COM, *supra* note 1.

[72] *Cf.* Whit Allen, *Power-Grid Independence Means Better Homeland Security*, Global Energy Network Institute, (Jan. 14, 2003) (discussing a risk analysis study which found that "even robust back-up systems incorporating multiple devices (e.g., dual power feeds from the electricity grid, batteries, diesel generators, UPS devices, etc.) run a 67 percent chance of failure over their lifetimes"), *at* http://www.geni.org/globalenergy/library/media_coverage/EnergyCentral/EnergyPulse/Power-Grid-Interdependence-Means-Better-Homeland-Security/index.shtml (last accessed Apr. 24, 2005).

transmission and support system maintain power – the end user must also have a source of backup power.

4. Interconnection Expands Speed & Range of Malicious Attacks

In March 2002, the NSTAC observed the following:

> [A]s the U.S. economy becomes ever more tightly connected through telecommunications, electronic signaling systems, power generation, information lines, financial connections, transportation nodes, and other connections involving critical infrastructures, possible disruptions have a far greater potential than ever before to ripple through the economy.[74]

One of the greatest drawbacks to the modern economy is the speed and distance at which problems can percolate; thus, "[p]roblems that might have been local disturbances [can] propagate through the entire interconnected system" before they are remedied.[75] The effects of interconnection on data networks are particularly acute: "[a]n attack on any of the approximately 96,000 networks interconnected as the Internet could cripple that infrastructure, and with the size of the Internet doubling approximately every 24 months, the potential for attack grows."[76] VoIP compounds this problem because it adds yet another "on-ramp" for malicious agents to introduce disruptive forces into the interconnected system.[77]

Of course, networks are not just interconnected to each other; eventually, they "off-ramp" at businesses, homes, and other facilities.

[73] *See, e.g.*, Kiser & Collins, *supra* note 11, at 41 n.213 (discussing examples of VoIP backup power supply options, which range in use-life from thirty minutes to eight hours).

[74] NSTAC VATF Report, *supra* note 49.

[75] Randal C. Picker, Raising Transaction Costs and Network Security: Of Heterogeneity and Autarky 12 (Cambridge Univ. Press) (forthcoming June, 2005).

[76] NRIC Physical Security Final Report, *supra* note 59, at 49.

[77] *Cf.* NSTAC CTF Report, *supra* note 5 ("[D]eliberate attacks are a significant factor in the availability of Internet service today because all components are interconnected; and attacks can be mounted from anywhere in the network.").

Network disruptions, therefore, can cause cascading failures[78] in the industries and communities that they are connected with and that rely on dependable communications.[79] The net result of tying a non-secure infrastructure (such as VoIP) to a secure infrastructure is a weakened networked infrastructure.[80] The following section will analyze the potential for VoIP to affect two of the nation's most critical industry sectors: energy and finance.

B. VoIP's Vulnerabilities Could Create Cascading Disruptions in Other Critical Infrastructure Sectors

The National Infrastructure Advisory Council (NIAC) recently published a survey ranking the critical infrastructure sectors on which various industries were most reliant.[81] Telecommunications was ranked first or second for seven of the nine responding industries.[82] Significantly, the energy and finance sectors ranked telecommunications as the infrastructure on which they are most dependent.[83]

[78] "A cascading failure is a disruption in which one infrastructure causes a disruption in a second [infrastructure]." James P. Peerenboom et al., *Studying the Chain Reaction*, ELEC. PERSPECTIVES, Jan./Feb. 2002, at 26-27, *available at* http://www.naruc.org/associations/1773/files/eperspectives.pdf (last accessed June 24, 2004).

[79] *See* NRIC PHYSICAL SECURITY FINAL REPORT, *supra* note 59, at 54 ("Attacks against Network Payload could expose companies, cities, or even countries to severe and dangerous consequences, including disruption of emergency response and failure of systems such as air traffic control and energy sharing grids.").

[80] *See* NETWORK RELIABILITY AND INTEROPERABILITY COUNCIL VI, HOMELAND DEFENSE, FOCUS GROUP 1B, (CYBERSECURITY): SUMMARY REPORT AND PROPOSALS FROM CYBERSECURITY BEST PRACTICES WORK COMPLETED BY FG1B BETWEEN MARCH 2002 AND MARCH 2003, 8 (2003), *available at* http://www.nric.org/fg/charter_vi/fg1/FG1B_front_matter_and_proposals_FINAL_3-13-03.doc (last accessed June 14, 2004) [hereinafter NRIC CYBERSECURITY FINAL REPORT].

[81] MARTIN G. MCGUINN, NATIONAL INFRASTRUCTURE ADVISORY COUNCIL, CROSS SECTOR INTERDEPENDENCIES AND RISK ASSESSMENT GUIDANCE: FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL 94 (2004), *available at* http://www.dhs.gov/interweb/assetlibrary/irawgreport.pdf (last accessed April 4, 2005).

[82] *Id.*

[83] *Id.*

A rule of thumb in critical infrastructure protection is that "[s]ecurity is [only] as strong as its weakest link."[84] Thus, the vulnerabilities in VoIP discussed above could make it the new "weakest link" in the highly critical energy and finance sectors.

1. ENERGY SECTOR DEPENDENCY ON SECURE, RELIABLE COMMUNICATIONS

Voice and data communications are the infrastructures on which the energy industry is most reliant.[85] Data communications provide real-time status updates as part of the energy industry's Supervisory Control and Data Acquisition (SCADA) systems and are also used for remote control of automated devices.[86] Voice communications, meanwhile, are necessary to communicate with field personnel to perform functions that cannot be remotely operated.[87]

A disruption of the SCADA system can have severe consequences for regional economic security and public safety. For example, a June 1999 SCADA failure in the Pacific Northwest contributed to a pipeline rupture, causing a leak of over 270,000 gallons of gasoline that precipitated an environmental disaster, three deaths, and increased gasoline prices.[88] Furthermore, the systems employed to back up SCADA, including "microwave, long and short wave radios, satellite voice systems, [and] privately owned phone networks"[89] each have drawbacks that either limit their implementation or reduce their reliability during extended outage periods.[90]

[84] NRIC CYBERSECURITY FINAL REPORT, *supra* note 80, at 8.

[85] MCGUINN, *supra* note 81, at 94. *See also* MITRE, Electricity Technical Discussion, *at* http://www.mitre.org/tech/y2k/sectors/docs/ELECTRICITY_DISCUSSION.html (last modified May 19, 2003).

[86] MITRE, *supra* note 85.

[87] *Id.*

[88] *See* Peerenboom, *supra* note 78, at 24.

[89] MITRE, *supra* note 85.

[90] *See* THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE, FINANCIAL SERVICES TASK FORCE REPORT 17-18 (2004), *available at* http://www.ncs.gov/nstac/reports/2004/Financial%20Service%20Task%20Force%20Report%20(April%202004).pdf (last accessed July 13, 2004) [hereinafter NSTAC FSTF REPORT].

2. FINANCE SECTOR DEPENDENCE ON SECURE AND RELIABLE COMMUNICATIONS

The financial sector is highly dependent on the telecommunications infrastructure "to support core payment, clearance, and settlement processes of financial institutions."[91] A disruption of critical communications for just a few minutes could seriously affect institutions' ability to continue operations.[92] Furthermore, because of the highly interconnected nature of financial transactions, a disruption at one of the larger institutions, or of a communications network serving several institutions, could quickly ripple through critical financial markets.[93] For these reasons, "[e]nsuring uninterrupted telecommunications services is a critical component of the business continuity plan of a financial institution."[94] Financial institutions recognize the need for diverse communications mechanisms[95] to strengthen their networks' resiliency by avoiding single points of failure.[96] VoIP – which foists formerly independent data and voice onto the same transport channels – decreases diversity and thus could weaken financial institutions' security.

3. A VOIP CASCADING FAILURE HYPOTHETICAL

To drive home the significance of the VoIP's security implications, picture the following scenario. A world in the future – but not far in the future. Terrorists monitoring the global weather systems track a hurricane approaching the eastern seaboard. For months they have been disguising investigative network scanning tools as Distributed

[91] *Id.* at 1.

[92] *Cf.* Notice of Federal Reserve Board Sponsorship for Priority Telecommunication Services of Organizations That Are Important to National Security/Emergency Preparedness, 67 Fed. Reg. 72,957, 72958 (Dec. 9, 2002) (explaining that telecommunications services are considered "essential where a disruption of 'a few minutes to one day' could seriously affect continued operations on an NS/EP function").

[93] *See* NSTAC FSTF REPORT, *supra* note 90, at 6.

[94] *Id.* at 7.

[95] *Id.* at 17-18 (explaining that alternative communications technologies, such as satellite, laser, and microwave, could "aid in diversity assurance and telecommunications service predictability").

[96] *See id.* at 8-9.

Denial of Service (DDOS) attacks on SCADA systems which are now frequently deployed along the Internet backbone.[97] As the hurricane approaches, they stand ready to send a modified Blaster worm through the undetected back door they have planted in energy grids across the nation. The hurricane hits the Outer Banks. It takes down the power in eastern North Carolina, triggering an emergency notification in the North Carolina SCADA system – and the deployment of the modified Blaster worm, which cascades through the Regional Transmission Organization network. The East Coast has lost electric power.

Emergency services personnel attempt to respond, but cannot communicate because neither the Internet nor their VoIP phones will work – as a simultaneous Denial of Service attack has been launched on one of the most widely deployed VoIP network platforms.[98] Medical personnel likewise cannot communicate supplies and staffing need, and hospitals are rapidly overrun and stripped of anesthetics, sutures, and sheets.[99]

A key node in the military command and control communications system has been taken out by a strategically placed car bomb, forcing high-level government communications back onto the public network – which no longer works. The President cannot call the vice-President – or anyone else – to coordinate a national response.

[97] *See, e.g.*, Donald I. Wallace, *Smart Fields Come of Age with Internet-Based SCADA*, PIPELINE & GAS JOURNAL, Feb. 2004, at 27.

[98] The Pacific Northwest Economic Region – a public/private partnership composed of legislators, governments, and businesses in Northwestern U.S. states and Canadian provinces – conducted a table-top exercise in June 2002 that illustrated the lack of awareness concerning internet and phone dependence among industry and emergency response officials. This exercise, entitled "Blue Cascades," hypothesized a physical act by terrorists directed at disrupting the region's electric power resources, which caused follow-on disturbances in regional communications systems. *See* PACIFIC NORTHWEST ECONOMIC REGION, *supra* note 69, at 2. Following the exercise, participants acknowledged that they had "difficulty envisioning a situation in which they would lose telephonic *and* internet communication and lacked contingency plans to work around the problem." *Id.* at 4 (emphasis added). See, regarding Denial of Service attacks on VoIP systems, CONTINUITY CENTRAL, VoIP: Vulnerability over Internet Protocol?, *at* http://www.continuitycentral.com/feature074.htm (last accessed Apr. 4, 2005).

[99] In contrast to this doomsday prediction, there is in fact some recognition that VoIP phones should not be adopted by emergency personnel until they are proven as reliable as traditional PSTN telephones. *See, e.g.*, Hiltzik, *supra* note 16 (quoting Michael Van Norman, technology and development manager for UCLA's Communications Technology Services Department: "There may be some areas where the phones absolutely cannot go down ... like the hospital or our police and fire departments. So until these issues are worked out, we don't see Internet telephones as a replacement.").

Chaos breaks loose in New York City and Washington, D.C. Law enforcement calls for backup on the emergency responder point-to-point radio systems, which run on separate frequencies from the public network. Without electricity, however, traffic lights are no longer functioning and routes through the congestion of those attempting to leave the city cannot be found. Power company personnel cannot call one another to implement/coordinate repairs. The financial markets cease operations, causing a global economic standstill.[100] Even after response efforts *do* get underway, they are hindered by follow-on Internet attacks prepared by the terrorists in advance of the initial onslaught.[101]

Improbable? Perhaps. But less and less so. The bottom line: aggregated functionality may mean increased efficiency – but it equally means increased risk.

V. Conclusion: Next Steps for Improving Network Security

With the security problem thus identified, the natural next step is to examine possible solutions. While VoIP introduces new vulnerabilities to voice communications, the guiding principles for improving security – diversity, redundancy, and autarky – are fairly common in traditional telephony. The trend towards VoIP over *private networks*,[102] rather than over the public Internet, presents the opportunity to practice these principles. However, market forces pushing VoIP toward enhanced security may fall short of providing

[100] In August 2004, some of the world's most important money-movement networks – including FedWire – moved onto the Internet backbone. Hilary Kramer, *Cyber Fears on Fed's Web Plan*, THE NEW YORK POST, Aug. 15, 2004, *at* http://riskman.typepad.com/perilocity/2004/08/ (last accessed Apr. 5, 2005).

[101] A real-life example of a follow-on Internet attack occurred in the weeks after September 11th, during which the "Nimda" worm "contribut[ed] to communication congestion and delays experienced by emergency responders." NSTAC VATF REPORT, *supra* note 49.

[102] *See* Ellen Muraskin, *VOIP Is As Secure As You Make It*, EWEEK.COM, May 14, 2004 ("[E]nterprise IP telephony … takes place almost exclusively over managed data networks … [and] therefore should not be confused with 'Voice over the Internet,' which traverses the open, vulnerable medium[.]"), *at* http://www.eweek.com/article2/0,1759,1592801,00.asp (last accessed April 4, 2005). This trend is driven at least equally by private networks' enhanced quality-of-service compared with voice transport over the Internet. *See* Hiltzik, *supra* note 16 (discussing investment in private fiber-optic networks to circumvent the public Internet to avoid its bottlenecks).

optimal resiliency levels; government may need to deploy incentives to make up the "security gap."[103]

A. AN OVERVIEW OF SECURITY PRINCIPLES

Building a secure infrastructure does not simply entail preventing attacks on that infrastructure.[104] Preventive measures frequently cannot keep pace with technology that seeks to exploit known vulnerabilities;[105] as such, network managers tend to believe that malicious attacks are inevitable despite best efforts at prevention.[106] To build a more secure infrastructure to carry both voice and data, resiliency principles and architecture must be included as part of "basic design precepts" of the infrastructure.[107]

Resilient networks are the combination of multiple practices.[108] Foremost among these is network *diversity.* Telecommunications networks are diverse when data can travel separate paths to the same endpoint, such that the failure of one route does not impact another.[109] Diversity is often achieved by separating circuit paths and decentralizing facility connections.[110]

Redundancy is another method of improving network resiliency. Redundancy practices involve maintaining alternative means of telecommunications – such as satellite phones or microwave radios – as backups to primary communications networks.[111] As the

[103] NRIC PHYSICAL SECURITY FINAL REPORT, *supra* note 59, at 15.

[104] *Cf. id.* at 43 ("Prevention is an important aspect of any physical security plan, but that plan will only be successful when coupled with [other mitigation strategies].").

[105] *See* NSTAC VATF REPORT, *supra* note 49 (discussing the ability of hackers and other malicious agents to develop tools to target vulnerabilities before they can be patched).

[106] Ken Belson, *Hackers are Discovering a New Frontier: Internet Telephone Service,* N.Y. TIMES, Aug. 2, 2004, at C4. (discussing a VoIP expert's assumption that "natural or people disasters" are not a matter of "whether" they will happen, but "when").

[107] NRIC CYBERSECURITY FINAL REPORT, *supra* note 80, at 7.

[108] NORTEL NETWORKS, WHAT'S ALL THE FUSS ABOUT RESILIENCY? 2 (2004), *at* http://www.nortelnetworks.com/products/01/passport/8600_rss/collateral/nn106100-111003.pdf. (last accessed June 10, 2004).

[109] NSTAC FSTF REPORT, *supra* note 90, at 10.

[110] *Id.* at 4.

[111] *Id.* at 3, 17-18.

telecommunications industry transforms to the next generation all IP-based network, the legacy PSTN may serve as a sufficiently redundant network to preserve communications resiliency.[112] However, operational proficiency with the PSTN will likely decrease as IP-based voice communications come to dominate the telecommunications market;[113] thus, providers will need to invest in other equally capable redundant technologies.

Finally, significant (but costly) resiliency can be achieved by implementing autarky in networks. Autarky is the practice of isolating systems by severing their connection to a public network.[114] Autarky used to be a common practice for managing critical information systems.[115] In recent years, however, most key systems have moved into the international environment.[116] Isolating critical units from networks supporting VoIP would certainly decrease businesses' total vulnerability; however, this might also limit VoIP's capabilities (such as its web-based features and potential for integrated information management) that rely on interconnected data infrastructures.

B. INCENTIVES FOR SECURITY IMPROVEMENTS

VoIP service providers increasingly recognize that privately managed data networks provide the best potential for near-term

[112] *Cf.* NSTAC CTF REPORT, *supra* note 5 ("[B]ecause of their large investments in public switched telephone network (PSTN) infrastructure, carriers are initially leveraging the best of both infrastructures . . . .").

[113] *Cf.* MCGUINN, *supra* note 81, at 44 ("Many organizations, in making their early transitions to Internet-based models, kept in place legacy processes in the event a fallback was required. Over time, these processes became outdated, personnel were no longer proficient in them, or the support infrastructure was no longer in place to manage them.").

[114] Picker, *supra* note 75, at 5.

[115] *Id. See also* NRIC CYBERSECURITY FINAL REPORT, *supra* note 80, at 10 ("[By] [i]solating critical components and partitioning the network infrastructure into smaller, protected areas, the opportunity to critically affect an entire network is dramatically reduced and network reliability is increased.").

[116] One of the most recent – and significant – examples is the Federal Reserve Board's planned introduction of "Fedline Advantage," an internet-based system intended to "extend the use of web technology to provide access to critical payment services. . . ." *See* Federal Reserve Financial Services, *Fedline Advantage is on the Horizon*, FEDFOCUS, May 2004, at 1, *available at* http://www.frbservices.org/FedFocus/2004/FedFocus504.pdf (last accessed Sept. 17, 2004).

improvements in quality of service[117] and security.[118] The remaining question is how best to create incentives for business to incorporate the aforementioned security principles – diversity, redundancy, and autarky – into developing private networks.

Given the FCC's current reluctance to regulate, market forces will be a considerable driver defining VoIP's security profile. Customers that rely on nearly infallible communications will demand that VoIP meet or exceed reliability and security levels on the PSTN before abandoning legacy systems.[119] Other highly dependent clients will likely demand certain security baselines in their contracts with VoIP providers.[120] Additionally, as VoIP becomes ubiquitous and substantially replaces the PSTN, tort liability for failure to provide certain minimum services and security could prove additional impetus for enhancements.[121]

Despite these economic drivers, a "security gap" may yet remain between the level of protection demanded by the market and the level of protection necessary to safeguard national economic security.[122] The federal government could deploy several means to help close this gap. First, the government may wield its considerable purchasing power and demand baseline security measures in procurement

[117] *See* Hiltzik, *supra* note 16 (discussing companies' investment in private fiber-optic networks to circumvent the public Internet to avoid its bottlenecks).

[118] *See* FARNSWORTH, *supra* note 51 (observing that a well-designed, secure corporate network "provide[s] a strong foundation for the security of all ... IP applications, including telephony"), *available at* http://www.convergedigest.com/blueprint/ttp04/z4cisco1.asp?ID=141&ctgy=4 (last accessed July 8, 2004).

[119] *See* Hiltzik, *supra* note 16 (noting that VoIP reliability issues prevent adoption by entities such as hospitals, police and fire departments "where the phones absolutely cannot go down.").

[120] *Cf.* NSTAC FSTF REPORT, *supra* note 90, at 3 (discussing telecommunication carriers' practice of negotiating customer-specific diversity requirements in service contracts).

[121] *Cf.* Kiser & Collins, *supra* note 11, at 41 (discussing potential liability for VoIP service providers for failure to connect 911 callers to emergency centers, if these providers market themselves as "seamless substitutes for traditional telephone service").

[122] *See* NRIC PHYSICAL SECURITY FINAL REPORT, *supra* note 59, at 15. *See also* NSTAC FSTF REPORT, *supra* note 90, at ES-1 ("[M]any telecommunications networks would need considerable upgrades to support NS/EP [(national security / emergency preparedness)] functionality within their larger network frameworks. At the same time, the demand for such services is insufficient to allow the marketplace to support the specialized requirements of NS/EP functions on a wide-scale basis.").

contracts with VoIP providers, and in so doing help to establish the market for secure converged network services.[123] The government may also explore targeted tax incentives to encourage investment in security enhancements.[124] Finally, the government could mandate minimum network security requirements.[125] However, given that the market for VoIP services is still evolving, such requirements might be both premature and in fact harmful for the future implementation of such services.[126]

C. VOIP'S "WINDOW OF OPPORTUNITY" TO ADDRESS SECURITY CONCERNS

The good news in this discussion of VoIP's security issues and shortcomings is that the technology is still part of a nascent industry. A recent report found that while service is steadily expanding, VoIP telephones will not outnumber their traditional PSTN counterparts until at least 2009.[127] Thus, there is still time for best security practices to become established and entrenched as part of *standard* VoIP operating procedures. Failure to do so could have disastrous consequences.

[123] NSTAC VATF REPORT, *supra* note 49 ("As security standards are developed ... Government can help establish the market by specifying those elements in contracts and purchase orders.").

[124] NSTAC FSTF REPORT, *supra* note 90 (suggesting tax incentives as a viable approach to improve security).

[125] Such requirements could be implemented through the FCC's Title I "ancillary jurisdiction" authority. Philip J. Weiser, *Toward a Next Generation Regulatory Strategy,* 35 LOY. U. CHI. L.J. 41, 51 (2003).

[126] *See* NSTAC VATF REPORT, *supra* note 49, at app. E ("Until the standards for packet-based services are established ... and the Government's requirements in the evolving environment are certain, legislation or regulation is premature."). *See also* Powell Statement, *supra* note 6, at 7-8 ("If we do not create the proper regulatory climate in the United States, it is quite possible our [future VoIP] local calls will be routed through Canada and Mexico at cheaper rates, rather than through Kansas and Montana.").

[127] *See* Ellen Muraskin, *Report: VOIP Phones Won't Gain Lead Until 2009,* EWEEK.COM, June 18, 2004, *at* http://www.eweek.com/article2/0,1759,1614773,00.asp (last accessed Apr. 4, 2005).