T

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

CONVERGENCE
TASK FORCE REPORT

T

JUNE 2001

Executive Summary

Telecommunications carriers are implementing cost-effective packet networks to remain competitive in the evolving telecommunications marketplace and to support wide-scale delivery of diverse, advanced broadband services. However, because of their large investments in public switched telephone network (PSTN) infrastructure, carriers are initially leveraging the best of both infrastructures, resulting in a period of network convergence during the transition to the next generation network (NGN).

The President's National Security Telecommunications Advisory Committee (NSTAC) Convergence Task Force (CTF) examined potential national security and emergency preparedness (NS/EP) implications of this indeterminate, developing public network infrastructure. The resulting information, provided in the CTF Convergence Report, is designed to enable the President and NS/EP entities to make informed recommendations to address the ability of the evolving public network (PN) to reliably support NS/EP communications requirements. Specifically, the report addresses—

- Potential security vulnerabilities of converged networks including those of the control space

- The realistic possibility of widespread outages of converged networks (resulting from focused failures) and the associated implications

T

- Ongoing standards development efforts in support of NS/EP priority requirements in the converged network.

Analysis of these issues also addresses concerns expressed by prominent Government officials regarding the possible impacts of the evolving network environment on NS/EP communications. More specifically, at NSTAC XXIII, Mr. Richard Clarke, National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, expressed concern about the lack of understanding regarding single points of failure (e.g., physical or cyber) in the Nation's network infrastructure and the subsequent NS/EP implications. Furthermore, Dr. Neal Lane, former Director, Office of Science and Technology Policy (OSTP), in response to the June 2000 NSTAC *Information Technology Progress Impact Task Force Report on Convergence,* recognized that the changing network environment requires consideration of the possibility of widespread outages in converged networks and in the evolving NGN and its potential NS/EP implications. Dr. Lane subsequently requested NSTAC's assistance in considering those matters.

As a result of its analysis, the CTF believes the PSTN is becoming increasingly vulnerable as a result of its convergence with packet networks. The open environment of packet networks provides ample opportunities for individuals to gain access to, manipulate, and steal sensitive information transmitted via the PSTN.

Furthermore, the interoperation of the intelligent network of the PSTN with Internet Protocol (IP) networks via gateways presents additional vulnerabilities. Specifically, the unreliability of existing gateway screening capabilities, the lack of security guidelines for interconnection, and the lack of control and authentication mechanisms for network management traffic, are all matters requiring further attention. Malicious activity directed at signaling gateways could precipitate network disruptions and impact overall network availability and reliability. Moreover, the Internet Protocol does not accord higher priority to "in-band" signaling messages. As a result, network congestion might not be circumvented in converged networks by using conventional NS/EP priority access and transport mechanisms. Additional analysis related to these vulnerabilities is required to gain further understanding of possible consequences. Also, the scope of analysis should be broadened to include convergence of wireless data networks with the PSTN.

Possible remedies for these vulnerabilities include those discussed at a recent NSTAC and OSTP Research and Development Exchange. They include implementation of signaling firewalls at network gateways and embedded security capabilities that are defined through

standards. The CTF also believes that industry and Government must cooperate fully to address these vulnerabilities and implement subsequent remedial tools.

Regardless of the aforementioned vulnerabilities, the evolving NGN ultimately must offer the NS/EP community quality of service (QoS) and reliability, protection, and restoration (RPR) features analogous to those of the PSTN. To help achieve this goal, converged network security and reliability concerns must be properly addressed by developing an understanding of evolving network technologies and applications through coordination in various forums, such as the NSTAC and standards bodies. The Government must foster cordial working relationships with NGN carriers, such as Internet service providers (ISP) and competitive local exchange carriers (CLEC), and encourage their participation in NS/EP forums. Perhaps most importantly, the Government should specify security requirements in packet network-related procurements in an effort to attain network reliability commensurate with that of the PSTN.

As the NGN evolves and advanced, broadband services proliferate, the Government must remain actively involved in pertinent activities of standards bodies, helping define and ensure the consideration of NS/EP requirements. Such involvement will help encourage industry to address NS/EP requirements, including extension of NS/EP priority services (such as Government Emergency Telecommunications Service [GETS] and Telecommunications Service Priority [TSP]) to an IP environment as required, while concurrently attending to societal demands for advanced network services. These efforts would ensure consideration of NS/EP requirements early in network design processes, avoiding the need for costly retrofitting. The Government should continue participating in working group activities related to NS/EP issues. These include those in the Internet Engineering Task Force (IETF) Signaling Transport Group addressing decoupling of call control from bearer channels in packet networks and those in the International Telecommunication Union Telecommunication and Standardization Sector (ITU-T) addressing implementation of an International Emergency Preference Scheme (IEPS).

For its part, industry should strive to employ cooperative risk assessments to help mitigate converged network vulnerabilities. At a minimum, risk-based, policy-driven, and economically justified key remedies should be adopted to curb network threats. The best methods of addressing network security risks involve analyzing systematic risk and remediation measures, ensuring stakeholder commitment and cooperation, sharing best practices, and researching and deploying new security measures. Also, broad industry participation in the NSTAC, the Government Subgroup on Convergence and any other appropriate mechanism is important to facilitate effective information sharing on emerging

network vulnerabilities and to provide ongoing NS/EP recommendations to the Federal Government.

To further address emerging network concerns, the CTF examined the issues of points of failure and possible widespread outage occurrences in converged networks. Past NSTAC analyses supplied foundational material for this analysis. In previous reports, the NSTAC stated that the resilient features of the PTSN and the diverse architecture of the Internet makes it unlikely that any single point of failure would cause a regional or national network disruption in either infrastructure.

However, the CTF recognizes a fundamental change in the emerging PN, wherein network vulnerabilities and possible points of failure could impact *service* availability and reliability rather than creating network component failures. Services such as voice over IP and bandwidth reservation capabilities could be essential to NS/EP operations in the future and subsequently could be impacted by packet network weaknesses. Therefore, the Government should not become reliant on nascent IP services without thoroughly analyzing their potential vulnerabilities. Further analysis of this issue is required.

The CTF requested and also participated in a National Coordinating Center for Telecommunications (NCC) single point of failure exercise. The results of this exercise supported the findings of the initial NSTAC PSTN and Internet widespread outage reports. Participants concluded that a scenario could not be envisioned, even in the converged network environment, in which a single point of failure could cause widespread network disruption. The participants found it more likely that any potential single points of network failure would have only local or “last mile” impacts and that preventive and remediation measures would require end-user coordination with carriers to ensure the needed network diversity.

Despite the encouraging results of the exercise, the CTF believes definitive assertions cannot be made regarding the implausibility of a national-level network failure. Unknown potential network failure points could exist and result in unforeseen network disruptions and service outages. Detailed network data sharing between Government, industry, and academia is essential to further understanding the converging networks and achieving more accurate network modeling and simulation techniques to analyze vulnerabilities and their impacts. Additional exercises should be scheduled to further analyze the NS/EP implications of network vulnerabilities as the NGN evolves.

T

The transition to the NGN also requires adoption of a formal process for sharing network data and vulnerabilities to address Government NS/EP concerns as they arise. The Information Sharing and Analysis Center (ISAC) for telecommunications, located at the NCC of the National Communications System (NCS), could facilitate such a process. Specifically, industry and Government should utilize the ISAC for assessing threats and developing suitable risk-mitigation strategies. Furthermore, amid the increasingly complex PN environment, industry has indicated a willingness to investigate the need for formal plans to assist carriers in recovery efforts during disasters. Successful plans would likely involve use of coordinating mechanisms, such as private networks, and would rely on Government support for such mechanisms.

NSTAC Recommendations to the President

Recommend that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, direct the appropriate departments and agencies, in coordination with industry to—

- Specify network security, service level, and assurance requirements in contracts to help ensure reliability and availability of NS/EP communications during network convergence and in the developing NGN

- Ensure that standards bodies consider NS/EP communications functional requirements during their work addressing network convergence issues, including security of PSTN-IP network Signaling System 7 (SS7) control traffic and development of packet network priority services

- Plan and participate in additional exercises examining possible vulnerabilities in the emerging PN and subsequent NS/EP implications on a national and international basis

- Utilize the NCC-ISAC to facilitate the process of sharing network data and vulnerabilities to develop suitable mitigation strategies to reduce risks.

T

NSTAC Recommendations to the IES for Consideration in the NSTAC XXV Work Plan

Recommend that the IES—

- Examine the NS/EP security and reliability implications of the convergence of wireless data networks with the PSTN and traditional wireless networks

- Support the efforts of the Government Subgroup on Convergence as requested by the Government in accordance with NSTAC's charter

- Further examine converged network control space-related vulnerabilities, including those of signaling and media gateways, and analyze possible NS/EP implications.

I

Terms of Reference

Convergence refers to a 3-to-5 year period of NGN evolution during which traditional circuit-switched networks (including the Advanced Intelligent Network [AIN]) and IP-based data networks will coexist and interoperate to enable end-to-end transmission of voice communications, until packet-based networks subsume circuit-switched networks.

The Next Generation Network is a public, broadband, diverse, and scalable packet-based network evolving from the PSTN, Advanced Intelligent Network (AIN), and Internet. The NGN is characterized by a core fabric enabling network connectivity and transport with periphery-based service intelligence.

n the past, the public network (PN)[1] consisted primarily of the narrowband, mature, public switched telephone

network (PSTN) and separate Internet. Now, the PN increasingly consists of converged networks, the transitional stage toward next generation networks (NGN). Converged networks comprise circuit switched networks interoperating with broadband packet-based Internet Protocol (IP) networks. Compared with the PSTN, IP networks are less mature, less understood, less secure, and more feature rich. In this evolving network environment, industry and Government must strive to identify and remedy associated network vulnerabilities to ensure continued security, reliability, and availability of the communications capabilities of the national security and emergency preparedness (NS/EP) community. Furthermore, the ambiguities of evolving networks and the rapid pace of technological progress necessitate continual and swift industry and Government evaluation of concomitant NS/EP communications requirements and prompt implementation of solutions to satisfy those requirements.

The President's National Security Telecommunications Advisory Committee (NSTAC) gives the President the information to make informed decisions with respect to critical NS/EP communications. Once informed, the President can make recommendations to address the ability of evolving networks to reliably support NS/EP communications. Recently, the NSTAC's Convergence Task Force (CTF) began examining possible NS/EP implications of the evolving public network infrastructure. Specifically, the CTF is examining potential converged network security vulnerabilities, including those in the control space; the realistic possibility of widespread converged network outages and associated NS/EP implications; and standards development efforts to support NS/EP priority requirements in the converged network. The initial results of these efforts are provided herein to assist the President and Government in making informed decisions to fulfill NS/EP requirements in the near-term.

THE MOVEMENT TOWARD A NEW PUBLIC NETWORK

S

everal factors are influencing carrier business decisions to implement packet networks. Foremost, economic considerations compel carriers to employ a single packet network-based NGN to support both voice and data traffic.[2] It is no longer feasible to maintain separate networks for voice and data. Per-minute charges for voice services have dropped faster than minutes-of-use has risen. At the same time, bit-per-second use of data networks has increased faster than prices for access have decreased, which has increased revenue.[3] These trends combined with annual reductions in prices for IP network equipment enable carriers to maintain earnings required to build high-bandwidth networks.[4] However, because carriers have enormous investments in PSTN infrastructure, they must initially leverage the best of both infrastructures in support of new services.

T

Terms of Reference

Advanced services are those generally requiring digital information transmission rates (bit rates) that are significantly higher than the nominal 56 kilobits/second which can be transmitted through an ordinary, high quality telephone voice circuit.
(NTIA, Advanced Telecommunications in Rural America, 2000, p. 5.)

Broadband refers to the capability of supporting at least 200 kilobits/second in the consumer's connection to the network ("last mile"), both from the provider to the consumer (downstream) and from the consumer to the provider (upstream).
(FCC, *In the Matter of Inlet Competition and Broadband Reporting*, Report and Order, CC Docket No. 99-301 [rel. March 30, 2000] supra note 8, at ¶ 22.)

The increasing demand for advanced broadband services is another factor influencing migration to NGNs. According to a recent National Telecommunications and Information Administration (NTIA) report, advanced network capabilities and their sustained high data rates are becoming ever more important as businesses and consumers increasingly rely on the Internet and on sophisticated applications incorporating audio and video.[5] Furthermore, NTIA claims that availability of advanced telecommunications will become essential to the development of business, industry, and trade, as well as distance learning, telemedicine, and telecommuting; therefore, the rate of deployment has implications for the economic development of our Nation's communities and the welfare of Americans.[6]

From a business-case perspective, continued implementation of packet networks to support wide-scale delivery of diverse, advanced broadband services is necessary to secure carrier competitiveness in the evolving telecom marketplace. The open and distributed nature of packet networks also enables rapid deployment of applications and services, permitting carriers to satisfy customer demands/requirements more quickly than in traditional circuit-switched networks. This service creation capability, characterized as more edge-based, indicates a shift from the closed and centralized PSTN service creation model exemplified by the Advanced Intelligent Network (AIN). While IP networks might eventually enable a richer, more powerful suite of telephony services, carrier investment in deploying Signaling System 7 (SS7) makes it more practical to develop new services by leveraging existing SS7 capabilities than by building data voice services from scratch.[7] Therefore, carriers are currently seeking to bridge the control space of the disparate networks via gateways. However, the movement toward convergence of packet networks and the PSTN during transition to the NGN could present new network reliability and vulnerability concerns.

CONVERGED NETWORK VULNERABILITIES

I

n the evolving public network, it is difficult to define causative vulnerabilities and potential impacts. Because converged networks are based upon less mature and less secure packet

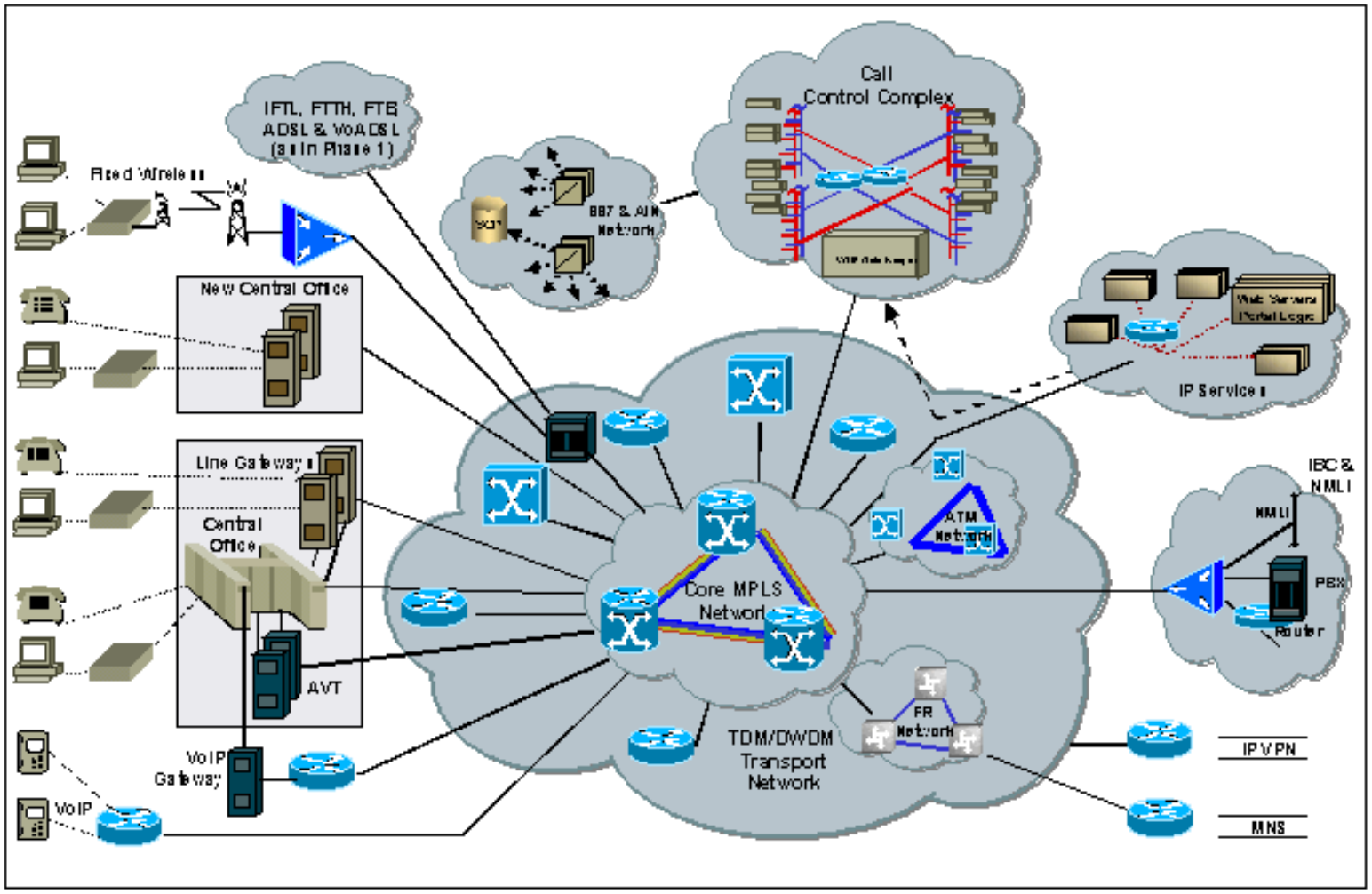
T

networks (when compared with the PSTN), the first challenge is to fully understand security weaknesses and the likely implications if those weaknesses are exploited. Therefore, to better understand industry views of the evolving public network infrastructure and potential associated vulnerabilities, the CTF obtained numerous briefings from industry representatives.

Understanding Emerging Networks

As indicated in Figure 1, the NGN will be a complex, diverse network. According to this depiction, the emerging NGN will unify multiple legacy and new services into a single backbone network consisting of IP running over an Asynchronous Transfer Mode (ATM) network using Multi Protocol Label Switching (MPLS).

Figure 1. Sample Depiction of an NGN Architecture



ATM is a network technology that supports multimedia communications such as realtime voice and video as well as data. MPLS enables IP-ATM integration, traffic engineering, and establishment of virtual private networks. MPLS also provides tools to engineer

quality of service (QoS) features into the network. This is important because in a converged PSTN-IP network environment, different services have different reliability, protection, and restoration (RPR) requirements, as well as different QoS requirements (e.g., throughput, latency, guaranteed delivery).

Essentially, services crossing multiple networks must rely on cooperation at each network-to-network interface (NNI) to provide end-to-end RPR and QoS. MPLS enables the policy-based networking needed to achieve this. Policy-based networking uses a network management paradigm with centralized databases for rules to enable distributed policy enforcement at the network element level. Such a system would help simplify operations with uniform control, translate service-level policy to network control functions, and permit scalability.

OPTICAL NETWORKING AND NS/EP

The era of optical networking has begun. By incorporating state-of-the-art wavelength division multiplexers in transport networks, it is possible to simultaneously send many information signals over a conventional optical fiber line. This technology has increased the usable bandwidth of these lines from 10 Gigabits per second to hundreds of Gigabits per second. Continuing advances in optical fibers and transport equipment will increase the number of possible high bit rate information signals that can be sent, making terrestrial Terabit per second optical fiber lines possible in the near future. But high capacity, high channel count systems are just one aspect of the emerging optical network. Individual network elements will be interconnected in sophisticated topologies and will function collaboratively to monitor network performance and to mitigate network failures.

The newest and most innovative feature of optical networks will be the capability to automatically establish optical connections, i.e., optical information transmission paths, using signaling methods similar to those in today's circuit switched networks. These Automatic Switched Optical Networks (ASON) will provide flexible end-to-end paths for broadband data and voice services such as IP-based and ATM-based services. Given the flexibility inherent in an ASON and the bandwidth it provides, these networks can serve as a powerful means for maintaining essential telecommunications services during emergency conditions or periods of network congestion.

Although ASON lies in the future, the enabling technologies are the subject of much current work within the telecommunications standards community, especially the T1X1 technical subcommittee in the United States and the International Telecommunication Union (ITU). Now is the time for ensuring that the options for emergency operations and secure access of optical networks are considered by the telecommunications standards community.
-Tobey Trygar, Telcordia

Other technologies, such as optical networking and wireless data networks will likely contribute to the composition of the NGN. Please see the insert above for a discussion of optical networks and Appendix A for information on the wireless Internet revolution.

The potential composition and functionality of emerging networks foretell a major challenge facing converged networks: synchronizing the high reliability, performance, and security standards established in the traditional voice network with those of data networks.

Switch reliability in today's PSTN is at 99.999 percent; on average switches experience less than 5 minutes of downtime per year.[8] Meanwhile, data network infrastructure (including access routers and core routers and switches) reliability is at 99.8 percent, resulting in a 17.5 hour-per-year average downtime.[9] It is reasonable to assume services such as automatic geographic location of 911 callers,[10] and priority access and transport features similar to Government Emergency Telecommunications Service (GETS) could transfer to packet networks. If this is the case, such networks must be reliable and secure to support mission-critical operations. Greater downtime could significantly interrupt NS/EP communications, as well as availability of NS/EP services. Therefore, to give the NS/EP community the levels of network and service reliability and security analogous to those of the PSTN in the evolving networks, many network technology and policy considerations need to be thoroughly vetted by industry and Government.

GETS gives NS/EP users priority access to local and long distance networks and specialized processing for NS/EP calls.

The first step in this process is to develop a more thorough understanding of evolving network technologies and applications through coordination in various forums such as the NSTAC and standards bodies. As this is achieved, associated vulnerabilities can be more readily identified through industry-employed mechanisms, such as risk assessments, so that the potential threats to NS/EP communications are fully considered and remedies instituted.

Establishing Risk Baselines

In adopting a framework for risk assessments, it is first necessary for each network provider to establish a risk baseline consisting of a defined set of parameters to help understand what potential risks exist and which risks, if any, they are willing to bear. For instance, one could posit that a network may be at risk if the network has vulnerabilities. Vulnerabilities may be unknown, or known and identified. Threats could exploit these vulnerabilities to damage that network. The measure of risk thus becomes a function of the potential damage and the level of threat. As vulnerabilities are identified, industry can determine their potential for damage and prioritize efforts to reduce the risks. As always, when industry makes essential decisions regarding what remediation to implement, the remediation's cost and complexity must be considered in parallel with the level of potential damage. Furthermore, any information in threat assessments from law enforcement or the intelligence community can be an important component in the remediation decision. Industry can use such threat information to prepare to mitigate known vulnerabilities.

A representative from a prominent infrastructure consultant described a methodology for

analyzing the security risks of converged networks. First, one must accept the notion that the PSTN is becoming increasingly vulnerable because of convergence with packet networks. Consequently, because the security measures implemented to protect these networks might not keep pace with technological growth, substantial risks are possible. These increased risks precipitate the need for systematic, cooperative risk analyses to help prevent PSTN and IP network outages from occurring.

Specifically, risk analyses of converged networks are necessary because network convergence exposes both voice over Internet Protocol (VoIP) users and PSTN users to new dangers. For example, deliberate 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. As a result, packet networks are subject to several fundamental security problems, including sniffing, spoofing, message altering, message duplication, message interception, and subversion of innocent hosts to multiply attacks. These vulnerabilities are extended to the PSTN as convergence occurs, wherein service disruptions and performance degradation could result from malicious acts such as denial of service attacks.

Additionally, the distributed nature of IP networks may increase the opportunity for cyber attack by allowing greater access to critical and enhanced PSTN systems.[11] The increased accessibility of packet networks enhances the potential for activities such as masquerading, wherein individuals could gain access to, manipulate, and steal sensitive information from PSTN components by using the identity of an authorized user.

Consequently, converged networks have additional sources of potential vulnerabilities that the PSTN alone does not have.

Converged Network Components

Signaling Gateway

A device that converts SS7 messages from the PSTN into various protocols required by packet networks and vice versa.

Media Gateway

A device that converts analog voice signals into various protocols required by packet networks and vice versa. Examples of media gateway devices include VoIP gateways.

Media Gateway Controller (MGC) (also referenced as a "softswitch")

MGC is a device that controls media gateways and provides call control and network resource management. The MGC integrates control functions (including the ability to process IP, digital subscriber line, ATM, and frame relay protocols in the same unit) and SS7 capabilities.

(Information referenced from www.techweb.com/encyclopedia)

Adequate risk assessments require examination of various converged network infrastructure components for potential vulnerabilities. Various types of gateways are used to link PSTN and IP networks and facilitate transition of signaling messages across the different platforms. These gateways also present a host of potential vulnerabilities. VoIP supporting gateways, for instance, could greatly increase the susceptibility of the PSTN to security breaches and network performance degradation. Techniques such as flooding gateways with spurious messages to disrupt their operations could impact communications across the networks. Also, by spoofing address sources, unauthorized individuals could access secure components of the PSTN via gateways. Moreover, the addition of these new components to an existing architecture and the resulting greater signaling traffic loads increase both the number of network elements that must be secured and the potential points of failure.[12] Therefore, establishing a risk baseline related to the gateways, identifying their critical vulnerabilities, and subsequently adopting securing mechanisms for remediation is of paramount importance to help ensure network reliability in a converged environment.

Securing the Control Space of Converged Networks

A major concern of the CTF is the interoperation of the intelligent network of the PSTN with IP networks via signaling gateways. As this occurs, IP networks could present those with malicious intent a "back door" into the control space of the PSTN, which could enable malicious activities such as insertion of false SS7 messages. If unauthorized parties gain access to a signaling gateway, they could disrupt or suspend its operations, alter its routing tables, or use it to forward false communications to other signaling gateways.[13] Such activities could precipitate network disruptions and impact overall network reliability and availability. Also, if the operations of a media gateway controller (with SS7 capabilities) were maliciously targeted, all customers whose service depends on that controller would likely experience service disruptions to include Enhanced 911 and NS/EP services.[14] Because the media gateway controller will likely play a critical role in the NGN, and because of its coordinating function among other network elements, security mechanisms are vital to sustain its reliability. Further investigation of potential controller vulnerabilities

is essential to fully understand possible NS/EP implications.

Another matter of concern involves the coupling of call control with bearer channels in packet networks. In the traditional PSTN, the SS7 network is an out-of-band signaling system that provides call setup and call services separate from the actual transport of the voice data. However, in 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.[15] In a converged network, such events could impact availability and reliability of the GETS service, which relies on the signaling network for functionality.

The Government should closely monitor standards bodies' efforts to address decoupling of call control from bearer channels in packet networks, including those of the Internet Engineering Task Force (IETF), ITU Telecommunication Standardization Sector (ITU-T), and International Softswitch Consortium.
A recent NSTAC and Office of Science and Technology Policy sponsored Research and Development (R&D) Exchange[16] addressed network control space vulnerability issues affecting converged networks. The exchange participants, including telecom and information technology (IT) industry members, and academia, commented that control space vulnerabilities could result from a number of factors. Primary causes cited include the inadequacy and unreliability of existing gateway screening capabilities, inadequate firewalls, the lack of security guidelines for interconnection, and lack of mechanisms to control or authenticate network management traffic and routing on the network.[17]
The attendees offered several solutions for such inadequacies including the following key preventive measures:

- Adopting effective gateway "signaling" firewalls
    - Ensuring embedded security capabilities are defined through standards
    - Ensuring producers of commercial-off-the-shelf security products are made aware of customer security requirements
    - Encouraging third party evaluation of products to ensure compliance with security requirements.[18]

The CTF concurs with these recommendations.

T

Coordination with Standards Bodies

Expanding upon the standards solution discussed at the R&D Exchange, the CTF believes current standards bodies' work regarding converged network reliability and security is of preeminent importance to NS/EP communications. The IETF has created various task force subgroups to address such converged network issues. Currently, the IETF Signaling Transport Group is studying how telephony signaling is carried over the Internet. It is important that Government, including the National Communications System (NCS), which is responsible for ensuring reliability of NS/EP communications,[19] be actively involved in such groups, to ensure consideration of NS/EP requirements, including GETS.

The NCS is already contributing to activities of numerous standards bodies such as the European Telecommunications Standards Institute, Telecommunications and Internet Protocol Harmonization over Networks (ETSI TIPHON) group. ETSI TIPHON is examining several security issues related to convergence, including identification and authentication procedures for emergency calls, and issues related to cyber attacks and malicious intrusion into networks.

The NCS is also active in ITU-T efforts regarding recommendation E.106, Description of the International Emergency Preference Scheme (IEPS). IEPS recognizes the requirement for priority communications among governmental, civil, and other essential users of public telecommunications services in crisis situations. IEPS, which is similar to GETS, would give authorized users priority access to and transport of NS/EP-related calls on an international basis within the PSTN and integrated services digital network (ISDN) infrastructures. A goal of the ITU-T is to encourage integration of IEPS services through execution of service level agreements (SLA), with service providers using standard capabilities inherent in the infrastructure. In other words, the current standards efforts seek to avoid costly retrofits for service providers (as realized through GETS) and encourage business practices whereby customers pay only for those services received. Moreover, if demand for such services materializes, service providers might be able to identify a market for priority services beyond the scope of Government NS/EP telecommunications (e.g., priority telecommunications services for doctors).

The NCS notes that numerous issues related to extension of IEPS to IP networks are also being addressed by standards bodies like the IETF.[20] Issues include identifying packet flows for IEPS, interfacing emergency communication processes in existing telephony services with IP-based services during convergence, and adopting a broad range of emerging IP-based services (e.g., electronic mail and instant messaging) to enhance IEPS operations. The NCS expects that security measures for protection of IEPS

communications (e.g., authentication), protection of the data stream, and procedures and processes for handling IEPS communications will have to be developed.

The CTF agrees that the Government needs to carefully consider several standards-based issues as the converged network emerges, including the business case for implementing NS/EP services in this environment, how the services would be deployed, and how supporting SLAs would be developed. The NCS will continue to support these efforts.

Ultimately, as major standards bodies recognize NS/EP priority requirements, it is important to ensure they become part of new standard interface requirements so that GETS calls, for instance, can continue to be recognized during network migration and convergence, and to avoid costly and insecure retrofitting of requirements.

As the NGN evolves and as advanced services and broadband networks proliferate, the Government will need to continue working closely with industry and standards bodies to forge an understanding of NS/EP requirements in general, to encourage industry to recognize a need for balance between societal demands for services and the needs of the NS/EP community, and to ensure requisite NS/EP standards are defined and deployed.

ADOPTING SOLUTIONS

Based on the information obtained from industry as outlined above, the CTF believes a dichotomy exists between societal and governmental requirements for emerging converged and broadband network services, such as VoIP. Carriers are quickly implementing packet networks to realize cost savings and to remain competitive in the rapidly evolving telecom market. As a result, every possible reliability and security implication cannot be fully realized and mitigated. Also, at this time, many users are willing to accept certain network reliability and security deficiencies in exchange for use of advanced and “free” or economic services, such as streaming video and VoIP. Conversely, from the NS/EP community perspective, there is a need to harmonize the high reliability and security capabilities afforded over the PSTN with those of the converged networks to ensure reliable end-to-end mission-critical NS/EP communications capabilities.

In today’s competitive telecommunications environment, the need for rapid innovation and the lack of a clear return on investment for network-based, NS/EP-related services often

preclude consideration of these services during technology development. In addition, competitive local exchange carriers' (CLEC) and Internet service providers' (ISP) lack of familiarity with traditional network capabilities and a working knowledge of technical capabilities related to NS/EP services introduces another element of uncertainty to the process. Therefore, the CTF believes it is important to inform these industry parties about the importance of NS/EP services and requirements and encourage them to participate in such forums as the NSTAC to promote cordial working relationships.

Also, the CTF believes industry should at minimum attempt to adopt key remedies that are risk-based, policy-driven, and economically justified to help curb network threats in general. These remedies might stem from a defined set of baseline needs related to physical and environmental concerns (i.e., the network framework), personnel concerns (i.e., insider threats), and technical aspects of emerging networks. The CTF realizes, however, that network risks must be prioritized according to the severity of the threat and associated mitigation costs, and it might not be feasible to justify expenditures required to alleviate certain risks.

In addition, carriers and network hardware and software vendors alike can employ various mechanisms to help facilitate near-term remediation. For instance, software architects can define processes for security tracking and maintenance. Service providers and equipment vendors can define operating environment requirements for call management agents and identify platform configuration requirements. Also, implementation of security mechanisms such as installation of firewalls for VoIP applications, signaling protection mechanisms such as encryption, and access control and non-repudiation features are all important factors.

From the Government's perspective, issues involving the reliability and security of GETS in a converged network environment must be resolved. Because it was designed to operate in the PSTN, GETS might not function optimally in packet networks. Furthermore, despite efforts to augment GETS operational processes and security and reliability mechanisms for such networks, the rapid pace of technological network advances will likely require constant implementation of requisite features to ensure continued GETS functionality. However, unless similar priority features, with parallel ability to meet NS/EP functional requirements, are implemented in packet networks, it might prove riskier to abandon GETS than to try to augment it for use in the NGN.

It is important for Government to further examine issues related to convergence to ensure NS/EP requirements are satisfied as the transition to the NGN continues. In relation, in its

December 2000 report, the Government's Convergence Task Force (USG CTF) recommended the establishment of a Subgroup on Convergence to examine NS/EP implications of the expanded capability and opaque reliability of the emerging NGN.[21] Their concerns should be fully articulated to industry to make certain they are considered as the NGN infrastructure is developed.

Similarly, industry, through mechanisms like the NSTAC, should continue drawing upon its knowledge of emerging network vulnerabilities, including control space security issues, to provide ongoing NS/EP-related advice and recommendations to the President.

In summary, the best methods of addressing network security risks are to analyze systematic risk and associated remediation measures, ensure stakeholder commitment and cooperation, share best practices, and research and deploy new security measures.

Also, tabletop exercises, wherein industry responds to hypothetical network vulnerability and outage scenarios, are effective for identifying possible issues of concern to the NS/EP community. The CTF participated in such an exercise to analyze the possible consequences of converged network vulnerabilities. The findings of the exercise are noted in the following section.

COULD CONVERGED NETWORK VULNERABILITIES LEAD TO A WIDESPREAD OUTAGE?

A

t the June 2000 NSTAC XXIII meeting, Mr. Richard Clarke, National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, expressed concerns about potential single points of failure, both physical and cyber, in the Nation's evolving network infrastructure. He questioned whether such points of failure, if exploited, could have the potential to cause widespread network disruptions and subsequently impact NS/EP communications. Also, Dr. Neal Lane, former Director, Office of Science and Technology Policy (OSTP), in a letter to the NSTAC Chair, expressed concern that the changing network environment requires consideration of the possibility of widespread outages in converged networks and the evolving NGN as well as the potential NS/EP implications. The CTF considered both issues.

Types of Network Failures

T

The CTF believes there are severity points/levels in today's network with changing probabilities of failure depending on size: national-level failure; regional-level failure; local-level failure; and last-mile failure (see Table 1).

For the purposes of the discussion related to focused failures, the CTF addressed only national and regional-level failures. Local and last-mile critical points-of-service issues do not have the potential to create regional outages and should be addressed by each facility manager in conjunction with the local service providers. The CTF also supports the Government's Joint Program Office (JPO)—Special Technical Countermeasures (STC)[22] efforts to address potential local and last-mile issues in relation to NS/EP entities.

Likelihood of a Widespread Outage

In two reports,[23] the NSTAC addressed the likelihood of a widespread outage in both the public telephone network and the Internet in the context of national and regional level failures. These reports offered conclusions relevant to the CTF's current analysis.

Table 1. Types Of Network-Related Failures

National Level Failure	A national level failure is highly improbable with little possibility of occurrence. Network diversity diminishes the probability of a catastrophic failure, and to date, no single point of failure has been identified that could cause such an event. Nonetheless, the task force noted that no definitive assertions could be made regarding the probability of a national level failure; currently undetermined points of failure could produce unpredictable types of extended network failures.
Regional Level Failure	It is more probable and more possible for a single point of failure to induce a regional level failure, likely resulting in the isolation of a particular region from normal service. However, it is even more probable that multiple points of failure would cause a regional outage. Furthermore, network complexity could increase the risk of a regional level outage, especially one resulting from a physical or cyber attack on multiple points. The duration of such an outage is scenario dependent. For example, an outage caused by an earthquake might be significantly different from one caused by a hacker attack, in terms of range, duration, and overall impact. The impact of a regional level failure could range from thousands to hundreds of thousands of customers.
Local Level Failure	While local level failures are quite probable and possible, their impact and duration are limited. The reasoning for this conclusion is that networks are less complex at this level; and rapid response and recovery mechanisms, such as fiber rings, circuit reroutes, and self-healing networks, reduce the impact of single points of failure. As with regional level failures, outage duration is ultimately scenario dependent.
Last Mile Failure	Outages induced by single points of failure are most probable at the last mile level, especially those physical in nature. While such outages might be the least complex to deal with, longer outage durations are possible because physical infrastructure restoration is required, especially during natural disasters.

Widespread PSTN Outage

According to the initial report, while the PSTN's evolving technologies provide an expanding array of services and features and facilitate network robustness, these same

technologies can introduce vulnerabilities. Moreover, standards and interoperability testing play a critically important role.

However, the initial report noted that the U.S. telecommunications industry has designed the PSTN to preclude single points of failure above the local switching level through both logical and physical diversity. (In the past, most network failures resulted from design flaws, software failures, or human action.) Technologies such as Synchronous Optical Network (SONET) rings and dynamically controlled routing, coupled with the diversity of carriers, result in a high level of public telephone network reliability and robustness. These resilient features mitigate the potential for any single point network failure resulting in a widespread outage of PSTN service. This notion is illustrated by carriers' continuing success in providing reliable service, even during natural disasters and power failures. The February 2001 Washington State earthquake demonstrated PSTN robustness, in that relatively few PSTN disruptions were experienced.

Widespread Internet Outage

TERMS OF REFERENCE

Single Point of Failure. A class of failure, solitary in nature, which is deemed to have the potential to cause a disruption that could have a major impact on regional or national network operations and services.

Widespread Outage. NSTAC discussed network outages in its December 1997 *Widespread Outage Subgroup Report*. A widespread outage is defined as a sustained interruption of telecommunications service that will have strategic significance to Government, industry, and the general public. Such an outage would—

- Likely affect the telecommunications service in at least one region of the country, including at least one major metropolitan area
- Involve multiple carriers, affecting both long distance and local service, and significantly degrading the ability of other essential infrastructures to function
- Impact the availability and integrity of telecommunications service for at least a significant portion of a business day.

Service Outage. The 1997 NSTAC report focused on implications related to physical network component failures. However, the transition to packet networks introduces vulnerabilities that could lead to service outages caused by events other than physical network component outages. For instance, denial of service attacks could impact VoIP services.

In the second report, NSTAC highlighted the lack of best practices in critical Internet services, such as the Domain Name System (DNS). NSTAC concluded that the Internet's highly diverse architecture and complex interconnection agreements, consisting of thousands of ISPs, make it unlikely that any single-point failure of a node or transmission facility would precipitate a major Internet service disruption. For example, a recent software glitch led to the failure of 4 of the 13 Internet root servers; but the result was a "nonincident" that did not significantly affecting Internet users or Web sites. This robustness, however, has precluded the Internet industry from gaining any sort of experience in managing major outages. Although such an outage is unlikely, this inexperience coupled with the Internet's modest level of security could conceivably contribute to future major and lasting disruptions of Internet *services* and traffic

T

flows.

To date, no one has maliciously exploited the open access of the Internet to cause a widespread outage of converged networks. Nonetheless, a widespread outage is still possible due, in part, to logical single points of failure (e.g., software-related) in the networks. Internet service providers might consider such points as distinct parts. However, they most likely are actually shared network components. Where the potential for systemic failures might exist, the lack of knowledge regarding potential network vulnerabilities makes it difficult to precisely assess potential risks and their effects.

On the other hand, outages are more likely to be element-specific. For example, if an attack caused the NCS Web site to go down, the rest of the Internet might still function normally. From a diagnosis standpoint, users will see only the effect, not the cause of the failure. It should be noted, however, that very simple causes—like viruses—could produce widespread effects.

Converged Network Issues

It is important to note, however, that the movement towards the NGN is giving rise to a fundamental paradigm shift—the exploitation of packet network vulnerabilities could now adversely affect *service* availability and reliability, rather than network component isolation or failure (e.g., server or router, fiber route, failures). VoIP, video services, DNS capabilities, and services potentially essential to NS/EP operations, including bandwidth reservation capabilities and priority traffic routing, could be impacted by security vulnerabilities discussed earlier in the report. For instance, a denial of service (DOS) attack on a particular ISP could impede data traffic flows, Web site accessibility, and VoIP service availability and reliability. Such effects are even more important to consider because if network intelligence data is transported over the same infrastructure as the services, a cascading problem could occur wherein network operations are affected, possibly leading to a more wide-scale event.

Furthermore, as IP-based services evolve, additional vulnerabilities and reliability issues related to the services might arise. Therefore, it is important that the Government not become prematurely reliant on nascent IP services as the transition to the NGN occurs. Official procedures might need to be created to analyze service reliability in the context of packet networks before their adoption. Furthermore, specific service level and assurance requirements could be specified in Government contracts with carriers.

Single Point of Failure Exercise

To further analyze the issue of focused network failures and their consequent effects, the CTF participated in the planning and execution of an NCC exercise. Exercise planning focused on the destruction of a bridge on or near which network infrastructure supporting concentrated traffic from multiple carriers was collocated. In an attempt to expand the potential breadth of consequences, the actual exercise expanded the physical component to include the destruction of five bridges with network assets crossing multiple rivers in the Midwest. After analyzing impact on carrier networks from an end-user perspective, the exercise participants could not identify any service disruptions caused by such an event. Because of unaffected assets buried underneath the riverbed and automated traffic rerouting techniques, carriers were able, in the exercise, to effectively compensate for lost capacity. Even when compounded by a cyber-related event, in which Add Drop Multiplexers (ADM) functioning to reroute traffic were not operating properly, end-user service impact was not evidenced. Therefore, this scenario would not lead to a widespread network outage as defined by NSTAC.

It is relevant to add that participants could not readily envision a scenario, even in the emerging converged network environment, whereby a single point of network failure could cause widespread network disruption.

While the results of this exercise cannot definitely assuage every concern about focused network failures, they do support the findings of the initial NSTAC Widespread Outage Report regarding the robustness of the PN.

Understandably, participants acknowledged that unknown potential network failure points could exist and result in unforeseen network disruptions. Subsequently, as the evolution toward the NGN continues, additional exercises are needed to analyze other network vulnerabilities and any NS/EP implications. Participants emphasized that future exercises should consider interdependencies among the information and communications sector and other critical infrastructures, such as electric power and transportation, to fully analyze the breadth of potential impacts.

Local and Last Mile Impacts

Exercise participants emphasized that any potential single points of network failure, such as a telecom hotel or specific local switches, would likely have only local or last mile impacts

rather than regional or national consequence. From an NS/EP perspective, participants suggested that preventive and remedial measures for these local impacts require end-user coordination with carriers to ensure network diversity in support of their organization's operations. It was noted that JPO efforts in this area are integral in offering network redundancy and robustness considerations to NS/EP organizations to help them facilitate uninterrupted NS/EP communications.

The Telecommunications Service Priority (TSP) program was also mentioned as a protective network mechanism that NS/EP users could employ. TSP enables NS/EP organizations to make carriers aware of which circuits are critical for priority restoration when outages occur. Accordingly, the issue of continued applicability of TSP in a packet-based environment to support recovery efforts was mentioned. Currently, only common carriers are mandated to provide TSP service, and it applies only to circuit-based services. Extension of TSP-like services to support priority restoration of packet-based *services* was mentioned as a possible issue for future examination.

Hypothetical Scenarios

Despite the optimistic findings from the initial exercise scenario, some issues surfaced when hypothetical scenarios were introduced. For instance, certain complications arose if it was posited the ADM problem resulted from a hacker attack. Time and resources needed to identify the specific problem and remediate it via a software patch, for example, introduced elements of complexity and uncertainty into the process. Participants indicated that such an event likely requires assembly of individual carrier network subject matter experts and possibly extensive coordination across carriers to ultimately solve the problem. This hypothetical scenario also touched on the issue of how common software platforms shared among specific network elements could be attractive targets for malicious acts intended to result in widespread implications. Such concerns could be addressed in detail in future exercises.

A second, but unrelated hypothetical scenario was introduced, wherein 75 percent of all carrier transport networks were down due to an unspecified reason. Participants agreed that such an event (dependent in part on the cause) would likely have widespread impacts; and restoral efforts might be complicated by carriers' inability to communicate to coordinate solutions. Such an obstruction to reconstitution efforts, especially in light of the increasingly complex nature of emerging networks, stimulated discussion about the status of a formal national level restoral mechanism, which carriers could reference for guidance if such an event occurred.

T

The NCC historically has served as a coordinating mechanism for assisting carriers in restoral efforts during disasters and has established standard operating procedures to support such efforts. Industry indicated a willingness to investigate the need for updating and formalizing these procedures as part of a national restoral mechanism that reflects the changing network environment. Such a mechanism could then be exercised on a regularly and revised as required. For these future exercises, the notion that the NGN will comprise complex systems, resulting in potentially complex failure modes, should be taken into account.

Also, during analysis of the restoral mechanism, the use of supporting coordinating mechanisms such as private networks like the Alerting and Coordinating Network (ACN) maintained by the NCS for recovery efforts could be analyzed. Government support for such mechanisms could also be explored.

The Path Forward

Ultimately, the CTF realizes no definitive assertions can be made regarding how low the probability of a national-level public network failure is because undetermined points of failure could produce unpredictable types of network impacts. NSTAC's work to date has not indicated any single points of failure in national or regional domains. Realistically, the probability of a widespread outage due to such a failure may not be high. However, the potential impact on society of such an outage is enough to warrant its continued consideration. Accordingly, network modeling and simulation efforts and exercises should be continued to assist in identifying potential network nodal vulnerabilities. These efforts should include Internet nodes. Comprehensive network infrastructure information from industry would help to maintain as accurate a depiction of the evolving PN as possible and enable continued analysis of potential points of failure and resulting impacts.

The CTF realizes definitive assertions cannot be made regarding the implausibility of a national-level network failure because undetermined points of failure could produce unpredictable types of network impacts.

It should be noted, however, that input received from various industry organizations and Government agencies suggests it is *impossible* to depict and maintain a *real-time* picture of the entire public telephone network due to the sheer volume of network modifications and growth. Furthermore, it is even more impractical to emulate the Internet because of its ever-changing and complex network infrastructure and unpredictable traffic flow patterns.

T

These issues notwithstanding, detailed network data sharing among all concerned parties is essential for realization of a comprehensive understanding of networks, and subsequently, more accurate network modeling and simulation and exercise scenarios.

The importance of information sharing related to these issues cannot be overstated. Ultimately, a formal, coordinated, and dynamic process for sharing network data and vulnerabilities could help address Government concerns as they arise. The Information Sharing and Analysis Center (ISAC) for communications located at the NCC at the NCS could facilitate such a process. There, operating at a classified level as required, industry and Government could assess threats and develop suitable mitigation strategies to effectively reduce the risk. The NCC, with its 17-year history of successfully coordinating recovery from outages, should serve as an ideal model for the new ISAC activities.

CONCLUSION

V

ast carrier investments in legacy infrastructure, including signaling networks, necessitate interoperability of the PSTN and IP networks for the near-term. However, the convergence of these disparate networks during the transition to the NGN could present unique network reliability and vulnerability concerns.

Within this environment, carriers must strive to sustain the high level of reliability historically provided by the PSTN to ensure continued availability of NS/EP services and communications. Achievement of this goal requires coordination among industry and Government through various forums such as the NSTAC, exercise activities, and standards bodies. In these forums, a thorough understanding of evolving network technologies and applications can be socialized and associated potential vulnerabilities analyzed. Furthermore, vulnerabilities could be readily identified through mechanisms such as risk assessments so that the potential threats to NS/EP communications are fully considered and remedies subsequently instituted.

The CTF is particularly concerned about vulnerabilities in the control space of converged networks. The open environment of IP networks could present opportunities to access the control space of the PSTN, enabling malicious acts such as insertion of false SS7 messages. Such activities could generate consequences that include degrading network reliability and compromising security and availability of NS/EP services such as GETS.

Government and industry should strive to adopt solutions to help mitigate control space risks. Some solutions, as defined at the recent NSTAC R&D Exchange, include ensuring that embedded security capabilities are defined through standards and ensuring that producers of commercial-off-the-shelf security products are made aware of customer security requirements. Industry and Government should continue to analyze control space infrastructure vulnerabilities and associated remediation activities as network convergence continues. NSTAC in particular should continue to analyze this issue.

As the NGN evolves, the Government will serve an increasingly important role in working with industry and standards bodies to promote an understanding of NS/EP requirements, including priority services, and to facilitate development and deployment of requisite NS/EP standards. Participation in standards bodies is of paramount importance as security considerations and other NS/EP requirements must be recognized and considered early in any network design process so that retrofitting is avoided.

Industry and Government should also continue analyzing the potential for focused failures in converged networks that could result in network and service outages. NSTAC indicated in previous studies that widespread outages of the PSTN and Internet were unlikely due to the robustness of these infrastructures. This notion was further supported by the findings in the NCC single point of failure exercise. However, the CTF realizes *definitive* assertions cannot be made regarding the implausibility of network failures within the emerging converged networks. Furthermore, as the NGN evolves, the exploitation of packet network vulnerabilities could adversely affect *service* availability and reliability, including services essential to NS/EP operations. Therefore, it is important that the Government not become prematurely reliant on nascent IP services and consider creating official procedures to analyze service reliability in the context of packet networks. Government should also specify specific service level and assurance requirements in Government contracts with carriers. Furthermore, Government should specify NS/EP-related security, service availability and assurance requirements in IT and network-based procurements, as feasible, to help ensure the NS/EP community's needs are satisfied.

Lastly, during the transition to the NGN, it is essential that a formal, coordinated, and dynamic process for sharing network data and vulnerabilities among all parties be adopted. The NCC-ISAC is an appropriate forum to facilitate such a process.

APPENDIX A

THE WIRELESS INTERNET

WIRELESS IS BECOMING A PREFERRED INTERNET ACCESS METHOD[24]

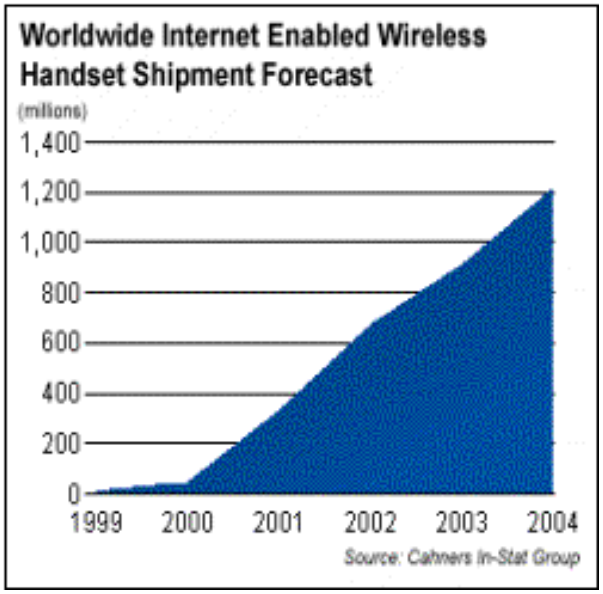
Wireless technologies are also contributing to fundamental changes in data networking, facilitating realization of truly integrated wireless data networks. Wireless devices (including palm computers, wireless modems, cell phones, and two-way pagers) will eventually displace the desktop personal computer (PC) as the preferred Internet access device, according to a new report by Cahners In-Stat Group. By untethering users, personal communications networks, wireless local area networks, mobile radio networks, and cellular systems harbor the promise of fully distributed mobile computing and communications, anytime, anywhere.

THE WIRELESS INTERNET. The usage rate of wireless Internet applications will likely explode in the near future with the commercial U.S. launch of high-speed 2.5 Gigahertz mobile technologies enabling rapid Web downloading, bandwidth-intensive file transfers, e-mail with large attachments, corporate intranet access, multi-user wireless gaming, and even streaming music from personal MPEG Audio Level-3 (MP3) services. See the Table A-1 for a description of wireless Internet technologies.

The new technologies—with names such as General Packet Radio Service (GPRS), Enhanced Datarate for Global Evolution (EDGE), and Code Division Multiple Access (CDMA) 1X—are widely expected to accelerate the use of wireless handsets as Internet-

access devices. The new technologies will increase throughput by as much as 130 Kilobits per second (Kbps) at launch. They will also help remove other deterrents to widespread adoption. Unlike most current wireless-data technologies, for example, the new technologies will deliver "always-on" digital packet-data connections, eliminating dial-up circuit-switched connections, expanding network data capacity, and-of critical importance to end users—eliminating a major source of battery drain. These technologies, however, are just the beginning. New Third Generation (3G) technologies,[25] defined by the International Telecommunication Union as delivering peak data rates up to 2 megabytes per second (Mbps) in stationary mode, are expected to launch commercially starting in 2002 under the wireless CDMA (WCDMA) and CDMA 1X Enhanced Version (EV) banners. The most robust version of CDMA 1X EV will eventually attain throughputs exceeding 1 Mbps, nearly matching digital T1 lines. With the launch of these 3G services, the selection of potential wireless-Internet applications will eventually grow to include even more bandwidth-intensive uses, some of a type yet to be invented.

The great potential for wireless Internet access is underscored by a forecast from market-research company Cahners In-Stat, which expects that in 2001, for the first time, worldwide unit shipments of Internet-enabled wireless devices including Internet-enabled telephones, two-way pagers, wireless modems, and wireless personal digital assistants, will exceed shipments of Internet-accessing PCs by a margin of 2:1. By 2004, they will out-sell PCs worldwide by a margin of almost 6:1. In-Stat projects that sales of Internet-ready wireless phones will surpass 1 billion annually by 2004, and by the end of 2002, virtually all wireless phones will be preloaded with Web micro-browsers. Users will be increasingly likely to rely on a single device rather than multiple devices for their wireless voice and data needs, the company added.



Beyond Business. Wireless Internet access device markets will see strong growth in the immediate future. Initially, mostly businesses and Government will use these devices. Currently, average consumers are deterred by slow transmission speeds, small screen sizes, and the expense of services and devices. However, as these issues are resolved and costs decline, dramatic increases in use are likely. In time, the distinction between mobile computing devices and wireless telephones will blur. Eventually, wireless computing devices will displace PCs as the

preferred method for accessing data and the Internet throughout much of the world. Jeff Pulver, Chief Executive Officer of Pulver.com, has predicted that wireless networks revenues will exceed those of local wireline for the first time in 2003. Other recent industry predictions indicate that approximately 240 million people will use their phones exclusively for wireless data applications by the end of 2004. Similarly, the Yankee Group predicts that the wireless data market will jump from $1.8 billion in revenues annually to $13.2 billion by 2003. Undoubtedly, growth in the wireless data market will serve as a catalyst to speed convergence.

Challenges. Despite the promise, demand for wireless Internet services could short-circuit if carriers oversell their network capabilities early on. Initial handset limitations, limited bandwidth availability, radio frequency (RF) conditions, distance from cell sites, cell site density, and other factors will conspire to reduce the technologies' maximum attainable throughputs. Additionally, security and privacy are issues requiring resolution before wireless devices become the reliable, tether-free medium to access the Internet. These wireless data network issues will need to be thoroughly examined as the NS/EP community increasingly relies on wireless mechanisms for information sharing and other operational activities. The convergence of the supporting wireless packet networks with the PSTN should also be analyzed for potential vulnerabilities.

TABLE A-1. ACCESSING THE WIRELESS INTERNET

Technology Overview	Technology Examples	Maximum Data Rates	Actual Data Seen by End User
GSM (Global System for Mobile Communications) GSM is the standard digital cellular phone service used in 85 counties worldwide. GSM is an open, non-proprietary system that features an international roaming capability. It uses digital technology and a variation of time division multiple access (TDMA) transmission methods.	a) GSM Circuit Switched b) GPRS c) WCDMA	a) 9.6-14.4 Kbps b) 115 Kbps (8 channels) c) 2 Mbps stationary; 384 Kbps mobile	b) 10-56 Kbps c) 50 Kbps Uplink, 150-200 Kbps Downlink
CDMA (Code Division Multiple Access) A form of digital, spread spectrum cellular phone service that assigns a code to all speech bits. CDMA offers increased capacity and more efficient use of spectrum.	a) CDMA Circuit Switched b) CDMA 1X c) CDMA 1X EV DO d) CDMA 1X EV DV	a) 14.4 Kbps b) 144-153 Kbps c) 2.4 Mbps d) 3-5 Mbps	b) 90-130 Kbps c) 700 Kbps d) Over 1 Mbps
CDPD (Cellular Digital Packet Data) CDPD, also known as "Wireless Internet Protocol (IP)," is a means of sending and receiving packet data via mobile devices over the existing analog cellular network.		19.2 Kbps	9.6-14.4 Kbps (can vary depending on RF signal)
Mobitex (Cingular Interactive) A non-proprietary technology by Ericsson that supports IP-based mobile data applications.		8 Kbps	8 Kbps (10-second latency for average message)

DataTAC (Motient Network) Provides standard IP message routing between LAN-based host computers and wireless computers.		4-19.2 Kbps	1.2-10 Kbps
Metricom A high-speed wireless data company that offers Ricochet, a wireless system that delivers high-speed mobile data access.		176 Kbps	128 Kbps and over (high-speed modem) 28.8 Kbps (low-speed modem)
iDEN (Integrated Dispatch Enhanced Network) iDEN is a digital trunked radio system based on TDMA that provides integrated voice and data services.	a) iDEN Packet Data b) iDEN Circuit Switched	a) 19.2 Kbps b) 9.6 Kbps	a) 19.2 Kbps (3-5 second latency) b) 4.8-9.6 Kbps
TDMA (Time Division Multiple Access) A satellite and cellular phone technology that interleaves multiple digital signals onto a single high-speed channel.	a) Circuit Switched b) EDGE	a) 14.4 Kbps b) 384 Kbps Initial Rollout (Due to Timeslot) 64 Kbps Uplink	b) Initial Rollout in 2001-2: 45-50 Kbps uplink, 80-90 Kbps downlink 2003:45-50 Kbps uplink, 150-200 Kbps downlink
Analog Circuit Switched		9.6 Kbps	4.8-9.6 Kbps
Source: Gartner Group/Dataquest, Stamford, Connecticut			

[1] "The PN includes any switching system or voice, data or video transmission system used to provide communications services to the public (e.g., public switched networks, public data networks, private line services, wireless systems, and signaling networks)," *NSIE Risk Assessment*, December 1995.

[2] According to an IT consulting group, packet switching will eventually be significantly more cost-effective than circuit switching because of its simpler "connectionless" nature and its adherence to open development standards rather than proprietary architectures. (Jim Metzler, Packet Maga-zine, Second Quarter 2000, http://www.cisco.com/warp/public/784/packet/apr00/p60-cover.html).

[3] Brian Silver, "Circuit To Packet Migration," *Internet Telephony*, February 2001, p. 58.

[4] Ibid.

[5] NTIA, *Advanced Telecommunications In Rural America*, 2000, p. 2.

[6] Ibid.

[7] National Research Council, *The Internet's Coming of Age*, 2001, p. 163.

[8] Hank Kafka, *Next Generation Network Evolutionary Trends*, Briefing to NSTAC on October 18, 2000.

[9] NRC, *The Internet's Coming of Age*, pg. 81.

[10] Ibid.

[11] NRC, *The Internet's Coming of Age*, p. 81.

[12] *United States Government Convergence Task Force Report*, p. 13.

[13] NCS, *Security Implications of Next Generation Networks*, December 2000, p. 29.

[14] Ibid., p. 28.

[15] Telcordia Technologies, *Network Evolution and Convergence*, June 1999, p. 72.

[16] As part of its ongoing network security activities, the NSTAC periodically sponsors R&D Exchanges to stimulate a dialogue among industry, Government, and academia.

[17] NSTAC, *Research and Development Exchange Proceedings*, University of Tulsa, September 28-29, 2000, p. 9.

[18] Ibid., pp. 9-10.

[19] The NCS assists the President in exercising the telecommunications functions and responsibilities, and coordinating the planning and provision of NS/EP communications for the Federal Government under all circumstances.

[20] The International Emergency Multimedia Service, currently being discussed within the IETF, includes IP-telephony and expanded services over IP to benefit NS/EP communications.

[21] *United States Government Convergence Task Force Report*, December 29, 2000, p. ES-2.

[22] JPO-STC operates under the Assistant Secretary of Defense for Command Control Communications and Intelli gence within the Department of Defense Infrastructure Assurance Program.

[23] The NSTAC reports are: *Widespread Outage Subgroup Report*, December 1997, and *Network Group Internet Report: An Examination of the NS/EP Implications of Internet Technologies*, June 1999.

[24] Information extracted from *Mobile Internet Access Devices*: *Surfing the 'Net on the Fly*, December 2000, Cahners In-Stat Group.

[25] Bandwidth allocation in support of 3G wireless technologies is an important issue, especially for Federal Government agencies. Recent reports suggest that options for allocating radio frequency spectrum space to 3G wireless systems—without disrupting current federal users of the spectrum—are limited. Please see the National Telecommunications and Information Administration report, "The Potential for Accommodating Third Generation Mobile Systems in the 1710-1850 MHz Band," at the Web site: http://www.ntia.doc.gov/ntiahome/threeg/33001/3g33001.pdf, and the Federal Communications System Report, "Spectrum Study of the 2500-2690 MHz Band, The Potential for Accommodating Third Generation Mobile Systems," at the Web site: http://www.fcc.gov/3G/3gfinalreport.pdf.