28 October 2008

CSIS - Cyber Security for the 44th Presidency

Telecommunications Task Group Final Report

1. Intent and Scope

The Telecommunications Infrastructure of the United States is arguably one of the fundamental enablers of virtually all other critical infrastructures on which the nation depends. Comprised of the interconnected set of networks and facilities of the common carriers and communications/information service providers, as well as the many privately-owned or purpose dedicated extensions thereof, the telecommunications infrastructure is the electronic highway by which information is exchanged for virtually every purpose in support of any function. From a cyber security perspective, it is perhaps the most "critical" of the critical infrastructures, since it is the primary delivery mechanism for cyber attacks against any and all targets, including the other critical infrastructures. This paper describes the current status of cyber security within the telecommunications infrastructure, defines the interdependencies between the telecommunications infrastructure and the other critical infrastructures, and develops recommendations for expanding and enhancing the cyber security of the collective telecommunications infrastructure.

2. Overview of the Telecommunications Infrastructure and the Common Carrier/Service Provider Environment

a. Technology Landscape

While the concept of a "telecommunications infrastructure" is relatively simple, the embodiment of this concept today is extremely complex. The historic - and readily understood - model of local and long-distance telephone service provided by a few large companies regulated at the federal and state level in the public good has been supplanted in the name of innovation and competition with a wide variety of models - mostly unregulated in the traditional sense. Providers of wireless services, internet services, broadband services, applications and data hosting services, content and information discovery services, etc., have entered the marketplace in an endless variety of forms, frequently competing and partnering with the traditional "telephone" providers at the same time. Further, the boundary between information, information technology, and telecommunications services has become almost indistinguishable. It should be noted that while there are an extremely large numbers of service providers of all sorts and sizes, ranging from the giants - AOL, Google, Yahoo, YouTube, MySpace, etc. - to the myriad of small local ISPs and service resellers, they almost always rely in some way on the transport facilities of the few large facilities-based telecommunications carriers which operate in the United States: AT&T, Global Crossing, Level-3, Quest, Sprint, and Verizon.

While there are many and varied business models and communications services today - one thing has become common - the way voice and data are transported across the core of the telecommunications infrastructure. Through the forces of convergence, the global and nation telecommunications infrastructure is rapidly moving to an Internet-based model, with all of the varied traditional services now supported via the Internet Protocol (IP). Today, the core of global telecommunications infrastructure largely consists of a set of Autonomous Systems (AS), which are individual IP networks operated by a carrier or service provider, or sometimes a private entity. These Autonomous Systems are connected together through peering relationships to exchange IP traffic between systems. While the original Internet model relied on public peering locations as the dominant method for IP traffic exchange, convergence has dramatically changed that situation. At the heart of the global infrastructure is the all-IP Autonomous Systems operated by the major (Tier One) carriers/service providers, connecting directly with each other through private peering relationships. For example, AT&T's core IP network in the U.S. is a single Autonomous System, designated AS7018, connected through private peering relationships with 24 other major service providers. These relationships handle over 99% of the traffic in and out of the AT&T U.S. core, all in IP.

Today, routing between Autonomous Systems is done using the Border Gateway Protocol, which was developed by the Internet Engineering Task Force to allow the Internet to become a decentralized system. BGP is an Inter-domain Routing Protocol which allows routing of traffic between and through Autonomous Systems without a centralized control determining the path between the source and destination of the IP packets across multiple systems. BGP is considered the core routing protocol of the Internet, and the larger global IP infrastructure. The peering points between Autonomous Systems, and the BGP protocol itself, are essential to the function of the global telecommunications infrastructure.

Of equal importance for the function of the global information infrastructure is the Domain Name System (DNS), which provides naming and addressing information for routing of IP packets between Autonomous Systems. The DNS is operated by a loose confederation of private sector companies, under the sponsorship of ICANN, the Internet Corporation for Assigned Names and Numbers. To quote from their website "As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes. ICANN, a public benefit, non-profit entity, is the international organization responsible for the management and oversight of the coordination of the Internets domain name system and its unique identifiers. ICANN was created through a Memorandum of Understanding (MoU) between the U.S. Department of Commerce and ICANN to transition management of the Domain Name System (DNS) from the U.S. government to the global community. " Recent developments, such as the work by Dan Kaminsky announced at the July 2008 Black Hat Convention, have highlighted some of the vulnerabilities in the Domain Name System.

(See Attachment A for a conceptual diagram of the global telecommunications infrastructure.)

In this model, the Internet and the Telecommunications Infrastructure have become indistinguishable. Indeed most carriers consider Internet just one of the many services they provide over their IP core network, including switched voice, Voice over IP (VoIP), traditional data services such as ATM and Frame Relay, private line services, virtual private network services, Internet services, wireless and mobility services, broadband and direct subscriber line services (DSL), IPTV, etc. All the information is moved across the core backbone as IP packets, with edge devices converting the IP packets to and from the various service formats. Traditional circuit switches are rapidly being phased out by the carriers, in favor of the more flexible, IP-oriented soft switches and IMS (IP Multi-media Switch).

The facilities-based common carriers generally divide their network into three layers for management and control purposes. These are typically: Services, IP Core, and Optical. The various customer-facing transport services (Traditional services like Frame, ATM, Switched Voice, along with newer services such as VoIP, VPNs, etc) are derived from the IP below - e.g. ATM over IP, and managed at the Services layer. The Services layer is where support for multimedia, wireless, and peer-to peer services is being implemented via such capabilities as IMS (IP Multimedia Switching) , SIP (Session Initiation Protocol), and Advanced DHCP (Dynamic Host Configuration Protocol) Within the IP core, MPLS (Multi Protocol Label Switching) is used to control routing priorities, using OSPF (Open Shortest Path First) route selection, and many carriers are in the process of implementing dynamic route control using IRSCP based Control Points. At the Optical Layer today, dual SONET rings is the dominant technology, with the current OC-192 circuits being upgrading to OC-768, in parallel with the introduction of Ultra Long Haul technology to allow direct lightwave connection between network nodes without regeneration and repeaters. Ultimately, this will allow the carriers to move away from SONET Rings to a fully-meshed optical structure, carrying IP directly over lightwave.

To satisfy the rapidly expanding bandwidth demands of multimedia sharing and multiplayer, on-line games, as well as the growing demands of wireless users, the carriers have rapidly expanded their fiber-optic transport capability. Most major carriers now utilize OC-192 (10 Gbps) and OC-768 (40 Gbps) circuit paths in their backbone, and employ Multi Protocol Label Switching (MPLS) routing to enable traffic prioritization within their network. The fiber-optic cable is arranged in dual SONET rings to provide redundancy, with automatic switchover in case a cable is cut. Also, in the carrier backbone today, satellite is rarely seen, being used almost exclusively for specialty applications in broadband multipoint distribution and to provide connectivity to remote locations or for emergency communications.

b. Legal/Regulatory Considerations

In addition to the numerous factors pointed out above that contribute to the current state of, and perspective on, the telecommunications infrastructure, the legal and regulatory environment further complicates matters. As is typical, technological development outpaces the country's legal and regulatory systems that do not have the agility to quickly adapt to new technologies. Coupled with the convergence mentioned above, a situation exists where the stakeholders do not necessarily know if or how the law or regulations apply to them, and such important issues may not be decided by the regulators or the courts for a number of years. New media, new delivery capabilities, all being delivered over the same indistinguishable infrastructure, has led to confusion and calls for regulatory intervention, such as the establishment of "net neutrality" requirements and the application of traditional circuit switched regulations on new technologies like VoIP.

Historically, a clear delineation existed in the regulatory realm between internet services and telecommunications services, with the former being relatively unregulated and the latter (because of its longer and more monopolistic history) being much more regulated. Through various lobbying efforts and the impact of new technology on traditional telecommunications infrastructure, blurring between the two has developed and various concerns regarding the appropriate regulatory treatment for rapidly developing telecommunications services and infrastructure have been raised and are continuing to be addressed.

In the area of cyber security, concerns have involved a few distinct issues. First, Customer Proprietary Network Information (CPNI) has been an area of heightened activity over the course of the last couple of years. CPNI requirements regulate how service providers handle and secure customer information derived from the provision of telecommunications services. Due in part to wide-spread allegations of security breaches, much stricter requirements have been imposed by regulators and implemented by services providers. Also, regulators have generally expanded the applicability of these additional security requirements beyond traditional circuit switched services to include certain VoIP applications as well. Overall, regulators are continuing to examine these issues and continue to consider whether to adopt even more stringent security requirements. As a general matter, the regulators' actions in the area of CPNI have elevated service providers' sensitivity to customer information and their handling of such information.

Second, the notion of net neutrality (discussed in further detail below) has resulted in concerns that internet network operators could impose unequal treatment on certain internet applications, which could ultimately lead to additional security concerns. Although the Internet infrastructure by nature treats all packets relatively equally, a "fast lane" for delivery of certain services appeals to a number of diverse constituents. With a growing demand for large bandwidth services (e.g., content delivery, VoIP, real-time trading, etc.), vendors are stepping up with technology that can meet those demands, resulting in large bandwidth demands being placed on the internet infrastructure. This development, along with allegations that certain internet applications have been blocked or degraded for competitive or network operation management, has led to scrutiny from regulators and a push from some sectors for equal treatment requirements to be imposed on internet network operators. Some have contended, however, that such an imposition would divert efforts away from such important issues as reliability and security.[1]

Finally, a call for greater regulation has been fueled by concerns over new attack vectors (such as VoIP spoofing and eavesdropping), along with the corresponding inability of law enforcement to gain access to possible evidence due to new and varied services. Although the PATRIOT Act and the use of National Security Letters have provided law enforcement with some ability to acquire needed information, criticisms of existing U.S. law continue to mount. In comparison to certain other countries that have taken a "top down" approach to lawful access to new technologies,[2] the law in the United States (particularly CALEA) has evolved somewhat sporadically over time. As a result, U.S. law has been criticized as having "many flaws and certain historical incongruities. The many amendments are due in part to the fact that U.S. legislators had a specific type of technology in mind at the time when the scheme was originally implemented."[3]

While regulatory activity cannot necessarily meet the needs of all stakeholders, a balance needs to be sought that will allow new services to continue to flourish without crippling the ability of both law enforcement and the general public to use and access the information that each stakeholder needs. As a general matter, the regulatory system does not offer effective incentives or forced mechanisms by which the law and the regulators can quickly address regulatory issues associated with new technologies, including any potential security concerns. By their nature, regulatory changes typically operate at a fairly slow pace, caught in the bureaucratic system by which they must operate. This slower pace is amplified, and particularly problematic, in the telecommunications arena, where technological and industry developments occur at an incredibly rapid and ongoing pace. Naturally included in such rapid development are security vulnerabilities.

Increased pressure on regulators to quickly act to address regulatory (including security) issues surrounding new technologies or technological changes should be considered, as well as the adoption of modifications to the regulatory infrastructure, such as the imposition of specific procedures and timeframes for completion of those procedures. Without additional pressures or specific procedural changes, the regulatory efforts to address security issues involving new telecommunications technology and applications likely will continue to fall far behind of the developments in the industry and thus hamper future efforts to effectively and swiftly address any security concerns.

3. Future Drivers and Influences

As mentioned above, demands for bandwidth in the core transport infrastructure are expanding rapidly, and the facilities-based carriers are responding in a variety of ways.

---

[1] *See, e.g.,* www.pff.org/news/news/2006/020706kyletestimony.html.

[2] For example, in Canada several "Consultations" have been conducted on the topic, in order to develop an appropriate legal regime. *See* http://www.privcom.gc.ca/keyIssues/ki-qc/mc-ki-la_e.asp.

[3] *See* Dominique Valiquet, "Telecommunications and Lawful Access: II. The Legislative Situation in the United States, the United Kingdom and Australia", Government of Canada, Law and Government Division (February 28, 2006). Available at http://www.parl.gc.ca/information/library/prbpubs/prb0566-e.pdf.

Besides the obvious answer of expanding circuit capacity in the core, the carriers are also moving towards implementing a richer suite of traffic management capabilities. The dual ring SONET structure at the optical level is migrating towards a fully-meshed architecture. This allows traffic to flow directly between any two modes in the network as required to meet demand, and greatly increases the reliability and survivability of the overall network. At the packet routing level, MPLS is being augmented by a variety of intelligent traffic routing capabilities that sense both traffic loading in the network and the applications being run by the users to dynamically optimize the overall traffic flow. The core infrastructure is also moving to support both IPv4 and IPv6 packet structures transparently, as the users and applications gradually transition to IPv6.

Mobile users are growing rapidly, and the overall number of wireless users in the United States now exceeds the number of wired subscribers for the first time. As the number of mobile users increases, so does the demand for sophisticated multi-media capabilities. This increases demand for wider bandwidth in the radio portion of the wireless infrastructure, as well as in the core network. As mentioned earlier, the carriers are moving towards an IMS environment at the network edges to better handle the needs of the mobile, multimedia subscriber, as well as integrating the traffic and applications management of the mobile subscriber into the intelligent core network control fabric.

While the technical challenges in the future telecommunications infrastructure are formidable, they are identifiable and reasonably-well understood. Perhaps the most potentially "game changing" driver for the infrastructure and the communications business as a whole is the possibility that some form of "net neutrality" policy will be imposed, either through FCC regulation or future legislation. While there is no universally-accepted definition of what net neutrality actually means, some interpretations would drastically impact the very fundamentals of the telecommunications business from both a business and technical perspective.

4. Interdependencies:

a. Dependencies of other Critical Infrastructures on Carrier/Service Provider Infrastructure

It is difficult to identify any of our Critical Infrastructures that would not be severely impaired or unable to function altogether, if a significant portion of the telecommunications infrastructure would be unavailable for any considerable period of time. In general, information technology and its operations, from personal computers in homes and small businesses, to hosting servers in data centers, to large mainframes in financial institutions and manufacturing and distribution facilities will be unable to operate effectively, and all the things they manage or control will come to a halt. Further, prior to the rise of Internet and its technologies, many industries - pipelines, electrical power generation and distribution, railroads and other forms of transportation, chemical processing, etc. - maintained their own separate and isolated telecommunications capabilities for industrial control purposes. Today that is changing dramatically as sophisticated computer-based control systems have become the norm, and most companies find it is no longer economical to maintain their own communications infrastructure. In the federal government, many departments and agencies still maintain private networks for internal communications, but most instances are largely dependant on the underlying common carrier infrastructure. Further, few federal agencies can do their job without the ability to connect to the larger world As but one example, even though the DoD maintains a number of dedicated networks for Intelligence, Command and Control, and Logistics Support Purposes, significant portions of these networks ride over common carrier facilities, and the support functions in particular, must connect to the Internet to reach suppliers. Public safety systems at the state and local level are typically dedicated and separate systems, as in police and fire/EMS radio, but rely on the telecommunications infrastructure for interconnection - such as connections between radio repeater towers - or to provide 911 and other emergency calling functions.

b. Dependencies of Carrier/Service Provider Infrastructure on other Critical Infrastructures

While the overall telecommunications infrastructure is designed to be highly reliable and resilient, there are some basic requirements from other critical infrastructures to keep it functioning. First and foremost, the telecommunications infrastructure needs a continuing supply of electrical power. To deal with short-term interruptions of the electrical power supply, many telecommunications facilities are equipped with back-up batteries and/or motor generator sets to supply power. Battery back-up capabilities are normally sized to support operations for 24 hours or less. Motor generator sets can typically operate for several days, limited by local fuel storage capacities. In most cases, where there is an extended power interruption, the facility operator will have pre-existing arrangements for delivery of additional fuel supplies, but this can be problematic under certain circumstances. For example, in the aftermath of Hurricane Katrina, getting fuel trucks into New Orleans to re-supply generators in communications facilities that were undamaged and operating was impeded by the physical damage to roads and bridges, and by the uncertain security situation. In the face of a cyber attack that might interrupt electrical supplies for an extended period, lack of electricity at fuel terminals could prevent the filling of tanker trucks for delivery, unless the terminals themselves had backup power capabilities.

Also, while the telecommunications infrastructure is largely self-managing to minimize the impact of localized equipment failures or service interruptions, service will gradually degrade over time unless failed equipment is repaired or replaced. This means that the information technology - computers, routers, switches, cross-connects, etc. - which actually make up the telecommunications infrastructure must be available to replace failed equipment. It also means that the replacement equipment can be and gotten physically to where it is required via the transportation infrastructure, and that the humans required to install the equipment are alive and able to get to the location as needed.

5. Existing Cyber Security Mechanisms and their Adequacy/Effectiveness

a. Within Carrier/Service Provider Infrastructure

A continuing stream of cyber attacks of all sorts and levels of sophistication have become commonplace in the Global Telecommunications Infrastructure. Driven by their business interests, the Carriers and Service Providers all use a variety of cyber security strategies and technologies to protect themselves and their customers from this ever-increasing flow. As a matter of basic survival, all of the major carriers essentially separate their network management and control systems from their network transport in order to isolate the control layer and the infrastructure components themselves from attack via the transport layer. Given the prevalence of BOTNET-driven DDOS attacks, most of the large carriers monitor traffic flow within their networks to identify these attacks, and either block them directly or alert their end customers to the attack. A variety of strategies are also employed to gather information from the network, such as unusual activity in a specific port or protocol, and identify other types of attacks. Most carriers/service providers offer their business enterprise customers a variety of managed security services, including threat warning, vulnerability scanning, managed firewalls, virus detection, SPAM-blocking, and intrusion detection/prevention services. ISPs, in particular, will bundle desktop firewalls with other security services such as SPAM Detectors, pop-up blockers and parental web-site controls for their consumer and small business customers.

While each carrier maintains some level of understanding of what is happening within their network with respect to cyber attacks, the precision of this picture varies from carrier to carrier, based on the dollars and manpower that the carrier is willing to invest. Since cyber security is viewed as a competitive advantage by some carriers, they are frequently unwilling to share the details of their cyber security capabilities with others, particularly their competition. Further, the carriers are limited by legal and privacy restrictions on CPNI and other forms of information as to what data they can share with each other and with governmental authorities. Consequently, there is no common, real-time picture of what is happening in the global telecommunications infrastructure, and a very limited ability to coordinate response mechanisms. Further, the make up of the infrastructure itself, with Autonomous Systems connecting to each other to exchange traffic between peering points, together with the reliance on the Domain Name Server hierarchy to provide addressing for routing of traffic, presents an inherent set of vulnerabilities that no individual carrier or service provider can deal with.

A variety of mechanisms do exist for sharing of high-level information and to coordinate cyber-security and other activities among the telecommunication carriers and service providers and with the federal government. These include the Network Reliability and Interoperability Council, under the auspices of the Federal Communications Commission; the National Security Telecommunications Advisory Council, which is a Presidential Advisory Group for which DHS serves as Executive Agent; and the Network Coordinating Center and Telecommunications Information Sharing and Analysis Center, which are private/public sector partnerships under the auspices of DHS. The National Cyber Security Division of DHS also operates the U.S. CERT, which gathers and disseminates cyber security related information on threats and vulnerabilities, along with other private sector entities such as the SANS Institute. While U.S. CERT and SANS are more focused on the broader range of information technology threats and vulnerabilities, these are obviously closely linked to the activities and interests of the carriers and service providers in protecting their customers from cyber attacks. A more complete description of the various elements that exist for sharing of Telecommunications Infrastructure related information is contained in Appendix B.

b. Across Critical Infrastructures

Aside from individual cyber security relationships between the carriers and service providers and their customers within the various critical infrastructure sectors, there is very little capability to identify and respond to cyber attacks in real time. The primary vehicle for sharing cyber security-related information across the critical infrastructure sectors are the ISACs, the sector specific Information Sharing and Analysis Centers created under PDD-63. The Partnership for Critical Infrastructure Protection is a private sector entity which brings together the leadership of the individual, sector specific ISACs for the purpose of coordination and information exchange. A more comprehensive discussion of this structure is contained in Appendix B.

6. Key Cyber Security Issues

a. National Capability for Cyber Attack Early Warning and Response

Perhaps the most pressing "Presidential" issue with respect to cyber security for the telecommunications infrastructure, along with the other critical infrastructures that rely on it for their function, is the lack of a national cyber early-warning and response capability. As mentioned earlier, the telecommunications infrastructure is the primary vehicle for delivery of cyber attacks against critical infrastructure components, yet there is no comprehensive mechanism for rapidly detecting and analyzing attacks nor coordinating responses. The existing mechanisms and structures such as the ISACs are largely oriented to post-attack forensic analysis and information exchange, rather than real time attack detection and interdiction. Most carriers and service providers today collect cyber security information from around their network, but are unable and unwilling to share it because of both privacy/legal restrictions and competitive issues. To be sure, many components of this capability already exist in both the government and private sector, but they are not integrated in such a way as to allow the real-time exchange of attack-specific cyber-security information. As but one example, under the EINSTEIN program sponsored by the National Cyber Security Division at DHS, the U.S. CERT monitors IP Packet flow information at the Internet Gateways of several participating federal departments and agencies, looking to identify cyber attacks. The JTF-GNO, operating under STRATCOM, performs a like function for DoD networks via the CENTAUR program. A number of the telecommunications carriers perform similar functions at their network peering points and nodes, and have developed sophisticated tools for analysis of the data that they gather. However, none of this data (or the analysis tools) is shared between these entities today, so each is looking largely within their limited field of view, with no ability to create a common operational picture. An operational structure is clearly needed to serve as the clearing house for the exchange of cyber attack information and response coordination among the common carriers and service providers, other critical infrastructure operators, and the appropriate government departments, including DHS, DoJ/FBI, and the DoD. One possible functional model is shown in Appendix D.

Facilitating the real time exchange of cyber attack information will likely require enabling legislation, including modifications to the Electronic Communications Privacy Act of 1986 and the Telecommunications Act of 1996 to allow and encourage the exchange of information by the carriers and service providers as well as address the privacy concerns.

One possible operational model to address this issue is the creation of a quasi-public corporation to serve as the clearing house for the exchange of cyber attack information and response coordination among the common carriers and service providers, other critical infrastructure operators, and the appropriate government departments, including DHS, DoJ/FBI, and the DoD. Other models are possible, such as the creation of an FFRDC or housing the function in a Government Department or Agency, but the quasi-public corporation presents significant advantages in establishing a clear legislative foundation and mandate, along with the required funding. It also has the most transparency and ability to gain the trust of the private sector and privacy advocates. The quasi-public corporation would be managed by a Board of Directors made up of senior representatives of the participating carriers and service providers, in addition to representatives for appropriate government agencies and public interest/privacy groups.

b. Streamlining the Public/Private Relationship & Structure

Over time, and with noble intent, a rather complex and overlapping structure of Committees, Councils, Associations, Boards, and other Groups have been established to address the intertwined issues of Homeland Security, Critical Infrastructure Protection, and Cyber Security. These are sponsored by a number of Government Departments, Agencies, or Offices, and in various forms from the varying perspectives of the various stakeholders. Appendix B gives just a partial list of these groups. While ostensibly performing essential functions, the shear number of these groups and the lack of overall coherence between them both reduces their effectiveness and makes any significant progress in cyber security problematic. A streamlining and consolidation of these groups into a few entities with well-defined and complimentary functions is badly needed. This could be accomplished as part of b. above. Likewise, there is a plethora of Federal Departments and Agencies - or multiple elements thereof - that have some stake in cyber security, critical infrastructure protection, or homeland security. This makes it extremely difficult and confusing for any private sector entity to engage with the "government" on a consistent and substantive basis on any aspect of cyber security.

c. Articulation of role of the FCC and the Regulatory Process for dealing with Cyber Security Issues in the Telecommunications Infrastructure

As discussed in the sections above, the landscape and structure for dealing with cyber security, homeland security, and critical infrastructure protection is complex and confusing. The FCC clearly has a role in regulation of the telecommunications infrastructure, yet their responsibilities with respect to cyber security are fuzzy, at best. Further, regulatory issues with respect to new technologies being introduced into the telecommunications infrastructure may have a significant impact of cyber security. Therefore, the ability for the regulatory process to react quickly but in a balanced fashion may be needed.

d. Hardening the Domain Name System and the Peering Points

While each carrier takes steps to protect their individual networks and their customers from cyber attacks, the Domain Name System and the Peering Points represent a significant vulnerability to the entire infrastructure - shared by all and owned by none. While a number of security improvements in the protocols used for peering and DNS access (BGP-4 and BIND) have been proposed, these have never been implemented, and there is no overall strategy or process for improving the cyber security of these essential components of the global telecommunications infrastructure.

e. Expanding Government Investment in Cyber Security Research and Development

A number of independent studies have pointed out the shortfalls in federal funding of cyber security research and development. In November 2002, Congress passed the Cyber Security Research and Development Act, which authorized expanded funding for cyber security R&D, but the funding levels authorized were never achieved. In 2005, the President's Information Technology Advisory Committee issued a report citing the criticality of increased cyber security R&D, but the recommendations were never implemented. In 2006, the GAO issued a report titled <u>Coordination of Federal Cyber Security Research and Development</u>. While not assessing the adequacy of R&D funding per se, the report noted that the federal research agenda recommended in the <u>National Strategy to Secure Cyberspace</u> had never been developed by OSTP.

In August of 2007, the President's Council of Advisors on Science and Technology (PCAST) issued <u>Leadership Under Challenge: Information Technology R&D in a Competitive World, An Assessment of the Federal Networking and Information Technology R&D Program</u>. The PCAST report stated: "The information infrastructure of the United States is a national asset, but it's seemingly endless, costly, and potentially dangerous vulnerabilities also heighten the Nation's overall level of risk. Once computing systems– including those that monitor and control critical infrastructures, including national security systems – are connected to the Internet, they can present openings through which attackers located anywhere in the world can enter, compromise systems, and steal or corrupt information. Despite intensive efforts in government and the private sector in recent years to identify and patch vulnerabilities and to upgrade overall security, attackers continue to find new avenues for attack."

The report included a summary of the 2008 Budget Requests relevant to information technology R&D, including cyber security and information assurance, from across the federal government. Of a total request of $3,061M, only about 7 percent - $218M - was requested for cyber security and information assurance. (How much of this requested funding is directly relevant to the cyber security of the telecommunication infrastructure and other critical infrastructures is unknown) The report cited the importance of expanding cyber security R&D, and urged the Office of Science and Technology Policy and the agencies that constitute the Networking and Information Technology Research & Development (NITRD) program, to increase their emphasis on cyber security R&D.

7. Summary and Recommendations

It is obvious from the forgoing that the United States faces a considerable challenge in enhancing the cyber security of the national telecommunications infrastructure. Despite innumerable studies, reports, plans, analyses, and recommendations, the cyber security problem continues to expand. The next administration, working on a bi-partisan basis with the new Congress, must act swiftly and decisively to change this course. We believe that the next Administration should proceed to develop specific, actionable recommendations for implementation in each of the five Key Cyber Security Issues discussed in Section 6 above.

Specifically:

a. National Capability for Cyber Attack Early Warning and Response

The next President should form a Task Group of Administration, Congressional, and Private Sector experts to develop a detailed concept and legislative proposal to implement the National Capability for Cyber Attack Early Warning and Response, as described above.

b. Streamlining the Public/Private Relationship & Structure
and
c. Articulation of role of the FCC and the Regulatory Process for dealing with Cyber Security Issues in the Telecommunications Infrastructure

The next President should form a Task Group to identify all of the various Elements of the White House, Departments, Agencies, Components of Agencies, Congressional Committees and Subcommittees, Regulatory Bodies (including the FCC), public/private committees, councils, and other bodies that have a role in cyber security, critical infrastructure protection, and homeland security, and develop recommendations for clarifying roles and responsibilities and streamlining the entire structure to make it more efficient and effective. This should include processes and structure for sharing of all forms of cyber security-relevant information, and the coordination of cyber security activities. The output of the Task Group should be a set of recommendations for streamlining the entire Public/Private structure, and a package of proposed Legislation and Executive Orders to implement the recommendations.

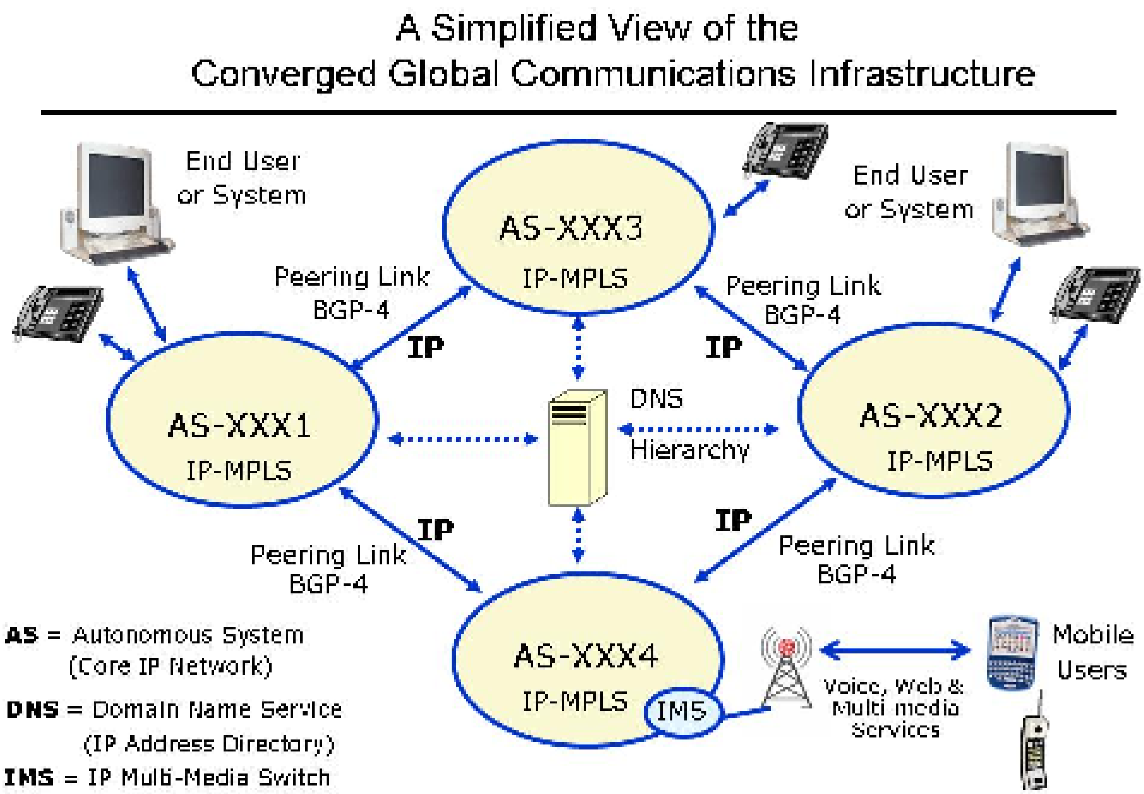
d. Hardening the Domain Name System and the Peering Points

The next President should charter a group of technical experts to define a set of options for increasing the security of the Peering Points and the Domain Name System against DDOS and other attacks. The options should include technical recommendations for near-term implementation to make immediate improvements, as well as a set of longer-term recommendations, including R&D activities. In parallel with the technical experts group, the next President should form a Task Group to review the current plans for privatization of ICANN by the Department of Commerce, and develop a set of recommendations to assure that the transition does not have a detrimental effect on U.S. interests, and that ICANN will, in fact, take definitive steps to increase the cyber security of the Domain Name System.

e. Expanding Government Investment in Cyber Security Research and Development

The next President should form a Task Group to develop specific recommendations for expanding federal investment in R&D specific to cyber security of the telecommunications infrastructure and other critical infrastructures. The immediate target is to double the current investment, with the increased funding going directly into R&R projects focused on the telecommunications infrastructure. This activity should be done in coordination with the activities of the Technical Experts Group examining long-term options for hardening the Domain Name System and Peering Points. The Task Group should also address streamlining the management process for federal investments in cyber security R&D, including the creation of and linkage to the federal research agenda recommended in the National Strategy for Securing Cyberspace. Methods for increasing coordination of government and private sector cyber security R&D activities should also be addressed in conjunction with the Task Group on the Public/Private partnership structure.

Appendix A



A Simplified View of the
Converged Global Communications Infrastructure
End User
or System
AS-XXX3
IP-MPLS
End User
or System
Peering Link
BGP-4
Peering Link
BGP-4
IP
IP
AS-XXX1
IP-MPLS
DNS
Hierarchy
AS-XXX2
IP-MPLS
IP
IP
Peering Link
BGP-4
Peering Link
BGP-4
AS = Autonomous System
(Core IP Network)
DNS = Domain Name Service
(IP Address Directory)
IMS = IP Multi-Media Switch
AS-XXX4
IP-MPLS
IMS
Voice, Web &
Multi media
Services
Mobile
Users

Appendix B

Communications Sector Partnership with Government

The Communications Sector has a long history of cooperation within the sector and with the federal government with respect to national security and emergency preparedness. This history distinguishes the Communications Sector from most other critical sectors identified in the National Infrastructure Protection Plan (NIPP). The sector personifies cooperation and trusted relationships that have resulted in the delivery of critical services when emergencies and disasters occur. A strong bond between the private and public sectors exists today in large part because of several organizations that were created in response to earlier threats to the nation's critical infrastructure.

National Communications System: The Sector Specific Agency for the Communications Sector is the National Communications System (NCS), currently housed within the Department of Homeland Security's Office of Cyber Security and Communications. The NCS was established by President Kennedy in the aftermath of the Cuban missile crisis when communications problems between the United States and key international players threatened to further complicate the crisis. Since 1963, the NCS has worked to strengthen the communications facilities and components of various Federal agencies, focusing on interconnectivity and survivability.

National Coordinating Center for Telecommunications: In 1982, telecommunications industry and Federal Government officials identified the need for a joint mechanism to coordinate the initiation and restoration of national security and emergency preparedness telecommunications services. In 1984, Executive Order 12472 broadened the NS/EP role of the National Communications System and created the National Coordinating Center for Telecommunications as a central public-private sector organization to coordinate response to emergency communications situations. In January 2000, the NCC was designated an Information Sharing and Analysis Center for Telecommunications in accordance with PDD-63. The NCC-ISAC facilitates information sharing among government and industry participants regarding vulnerability, threat, intrusion, and anomaly information affecting the telecommunications infrastructure.

The National Security Telecommunications Advisory Committee (NSTAC): The NSTAC was created in 1982 by Executive Order 12382. NSTAC provides another highly successful example of how the private sector helps direct government decisions around national security and emergency preparedness communications (NS/EP). This advisory committee to the President brings together 30 industry chief executives representing major telecommunications companies, network providers, information technology companies, finance and aerospace businesses. NSTAC provides industry-based advice and expertise to the President on a wide range of telecommunications problems related to implementing NS/EP communications policy issues. These include, but are not limited to, information security, information assurance, and critical infrastructure protection. NS/EP communications enable the government to make an immediate and coordinated response to all emergencies, including cyber attacks. NS/EP communications allow the President and other senior Administration officials to be continually accessible, even under stressed conditions. The impact of today's dynamic technological and regulatory environment is profound with new technologies and increasing competition bringing both new opportunities and new vulnerabilities to the information infrastructure. The NSTAC is strongly positioned to offer advice to the President on how to leverage this dynamic environment to enrich NS/EP communications capabilities and ensure that new architectures fulfill requirements to support NS/EP operations; and to avoid introducing vulnerabilities into the information infrastructure that could adversely affect NS/EP communications services. The NSTAC's current work plan includes issues ranging from information sharing and the security and reliability of converged networks to research and development (R&D) issues related to converged networks.

The Network Reliability and Interoperability Council (NRIC): Government-imposed solutions may hinder the ability of business to adapt and respond effectively to the changing threat environment. So it becomes critical for business and government to work collaboratively towards solutions that are meaningful, adaptable and sustainable. The voluntary development of and compliance with "best/sound practice" approaches to physical and cyber security is a model that is time tested. It is illustrated through the work of the Federal Communications Commission's Network Reliability and Interoperability Council. The NRIC is a successor to the National Reliability Council, first established in 1992. Through the work of seven successive councils, subject matter experts from business and government have come together to address network reliability and interoperability issues of concern, develop best/sound practices and encourage voluntary adoption. The NRIC will soon merge with the Media Security and Reliability Council (MSRC) to create a new organization, the Communications Security, Reliability, and Interoperability Council (CSRIC).

National Security Information Exchange (NSIE): In April 1990, the Chairman of the National Security Council's Policy Coordinating Committee requested the NCS Manager identify what actions industry and Government should pursue to protect critical NS/EP telecommunications from the growing "hacker" threat. The NCS Manager subsequently requested that the NSTAC provide industry's perspective on the network security issue. Ultimately NSTAC created a mechanism for security information exchange and produce a corresponding implementation plan. The NSTAC and NCS Manager also established separate, but closely coordinated, Network Security Information Exchanges (NSIEs). In May 1991, the NSIE charters were finalized, and NSTAC companies and government departments and agencies designated their NSIE representatives, chairmen, and vice-chairmen. The NSTAC and government NSIEs held their first joint meeting in June 1991. Industry and government coordinate through their respective NSIEs to voluntarily share sensitive information on threats to operations, administration, maintenance, and provisioning systems supporting the telecommunications infrastructure. Government NSIE members include departments and agencies that use national security and emergency preparedness (NS/EP) telecommunications services, represent law enforcement, or have information relating to network security threats and vulnerabilities. NSTAC NSIE representatives include subject matter experts who are engaged in prevention, detection, and/or investigation of telecommunications software penetrations or have security and investigative responsibilities.

Communications Sector Coordinating Council (CSCC): The Communications Sector Coordinating Council (CSCC) became operational in calendar year 2006. It was chartered to foster the coordination of policy initiatives to improve the physical and cyber security of sector assets, and ease the flow of information within the sector, across sectors and with designated Federal agencies. Through the CSCC, private-sector owners, operators and suppliers can engage Federal government entities to: identify and coordinate policy issues related to the protection of critical infrastructure and key resources; facilitate the sharing of information related to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices; and, address policy issues related to response and recovery activity and communication following an incident or event. The CSCC now embraces 35 member companies and has become more representative of the diversity of the Communications sector. Members include wireline, wireless, cable, satellite, information service providers, as well as commercial and public broadcasters, service integrators, and equipment vendors. Small and medium size companies are represented through CTIA, USTelecom, ITA and NCTA. CSCC members meet quarterly to review industry and government actions on critical infrastructure protection priorities, confer with Federal agency representatives, review cross sector CIP issues, and coordinate with industry participants in NSTAC and the NCC ISAC to ensure industry coordination. Council work groups meet frequently to engage industry and government SME's on task force initiatives. Top 2007 CSCC priorities included the sector's risk assessment of critical assets, cross sector pandemic planning and implementation of access and credentialing and emergency wireless protocols.

The CSCC and IT Sector Coordinating Councils maintain close coordination on a range of policy and operational initiatives. Both sectors participate in a recently formed cross sector cyber security work group. Both have worked to heighten industry's role in NS/EP exercises such as last summer's ESF2 exercise in New Orleans and in TopOff 4. In the aftermath of Katrina, the Councils met to discuss ways of strengthening industry preparation and response to major events. Both participate in ongoing sector risk assessment activity. Both organizations have elected sector liaisons to attend each other's coordinating council meetings and they meet annually to confer, with government counterparts, on ongoing sector activity.

Partnership for Critical Infrastructure Protection (PCIS): The Communications Sector Coordinating Council is a member of the Partnership for Critical Infrastructure Security (PCIS.), a private sector organization. PCIS is comprised of the leadership from each of the Sector Coordinating Councils, which represent the owners and operators of the critical infrastructure and key resources sectors identified by the government in HSPD-7. The mission of PCIS is to coordinate cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services. This mission encompasses physical, cyber, and human security that rely on strong infrastructure integrity and resilience. Accordingly, the PCIS mission spans the full spectrum of critical infrastructure matters from prevention, planning, and preparedness to business continuity, mitigation, response, and recovery. The PCIS has worked to encourage a productive industry partnership with the Federal government over the past six years. It was formally recognized as the Private Sector Cross-Sector Council in the National Infrastructure protection Plan when it was released in 2006. The NIPP states that the “cross-sector issues and interdependencies are addressed among the sector coordinating councils through PCIS. PCIS members, including the CSCC, continue to work with designated Federal agencies on implementation of their sector specific plans.

Communications Sector Specific Plan (CSSP): The CSCC completed work on the CSSP for critical infrastructure and key resource (CI/KR) protection, as recommended by the NIPP, in December 2006. The plan was subsequently released in May 2007. It was developed jointly by industry and the National Communications System, with input from Federal government agencies ranging from the US Department of Commerce to the Federal Communications Commission. The CSSP provides a framework for protecting the Nation’s critical communications assets and key resources. It addresses asset identification, risk assessment and mitigation, protective programs and government measurements.

The goals of the CSSP include the need to:

- Protect the overall health of the national communications backbone;
- Rapidly reconstitute critical communications services after national and regional emergencies;
- Plan for emergencies and crises by participating in exercises and updating response and continuity of operations plans;
- Develop protocols to manage the exponential surge in utilization during an emergency situation and ensure the integrity of sector networks during and after an emergency event;
- Educate stakeholders on communications infrastructure resiliency and risk management practices in the Communications Sector;
- Ensure timely, relevant, and accurate threat information sharing between the law enforcement and intelligence communities and key decision makers in the sector;
- Establish effective cross-sector coordination mechanisms to address critical interdependencies, including incident situational awareness, and cross-sector incident management.

The CSSP acknowledges the lead role played by private sector owners and operators in protecting critical assets. The communications companies that own, operate and supply the Nation’s communications infrastructure have historically factored natural disasters and accidental disruptions into network resiliency architecture, business continuity plans, and disaster recovery strategies. The interconnected and interdependent nature of these service provider networks has fostered crucial information sharing and cooperative response and recovery relationships for decades. The CSSP also articulates the role of the Federal government in providing the support and resources necessary to identify threats and help mitigate risk.

The Communications Sector's strategy is to ensure the nation's communications networks and systems are secure, resilient, and rapidly restored after an incident. The approach outlined in the CSSP includes:

- Defining industry and government roles in protecting communications infrastructure by leveraging corporate capabilities and government programs;
- Adopting an architectural approach to infrastructure identification and risk assessment processes;
- Coordinating with other sectors and customers on critical infrastructure dependencies and solutions for mitigating risk; and
- Working closely with DHS to advance sector protection and mitigation measures.

The CSSP defines the three major arenas where risk assessments are conducted: industry self-assessments; government-sponsored assessments and government-sponsored cross sector dependency analyses. Industry self-assessments of risk are ongoing. Such assessments are conducted to verify compliance with company policies, industry standards, contract agreements and regulatory requirements.

Appendix C

Some Attack Models against the Telecommunications Infrastructure

Today, routing between Autonomous Systems is done using the Border Gateway Protocol, which was developed by the Internet Engineering Task Force to allow the Internet to become a decentralized system. BGP is an Inter-domain Routing Protocol which allows routing of traffic between and through Autonomous Systems without a centralized control determining the path between the source and destination of the IP packets across multiple systems. (Note: While BGP makes the actual routing of packets independent of centralized control, an overall Domain Name System (DNS) hierarchy is still required to provide IP address information.) BGP is considered the core routing protocol of the Internet, and the larger global IP infrastructure. The peering points between Autonomous Systems, and the BGP protocol itself, are essential to the function of the Internet and the global infrastructure, and thus represent potential major points of vulnerability.

Any discussion of cyber security measures should be framed by “What are you trying to protect against?” While there is almost an infinite variation of cyber threats and attack methods ranging from crude to sophisticated, they can be generally be placed in but a few categories:

a. Saturation/DOS Attacks

This class of attacks attempts to overload the target or targets with a large volume amount of IP traffic, effectively blocking legitimate traffic from getting through or being processed. It includes such techniques as spamming to overload e-mail servers, and viruses and worms which infect a computer or other device and them propagate multiple copies of itself to other machines. The Sasser and Zobot worms and the MyDoom virus are some recent examples. These can target end computers or devices, application servers, and network components themselves, such as routers, or even Firewalls and Intrusion Detection Devices. In most cases, the objective is to deny service, but some types of worms or viruses can also damage or erase information files, or recruit computers into a BotNet. Sometimes these attacks are intended to make a social statement, or to establish a hacker’s credentials – other times they are used for criminal purposes to blackmail a specific target or targets.

b. Sophisticated Attacks against Network Infrastructure

On 6 February 2007, six of the thirteen Top Level Domain (TLD) servers, which are essential to the operation of the DNS hierarchy and the Global Telecommunications Infrastructure, were subjected to a Denial-of-Service attack in two waves. The first wave of the attack lasted approximately two and a half hours; the second wave lasted five hours. The DNS translates common network names, such as “att.com” or “osd.mil” into specific IP addresses for routing of packets to their destination. The TLD (or “root”) servers tell an inquiring computer where to go in the DNS hierarchy to get specific IP addresses for a particular domain. Of the six root servers attacked, two were seriously affected – one of which was the "G-root" server run by DoD in Columbus, Ohio to support the NIPRNET. While the analysis of the attack is still ongoing, it appeared to combine several familiar attributes – it originated in the Asia-Pacific region, it used some form of BotNet to generate a massive amount of queries to the six servers, and the attack itself was based on a brute force approach. This relatively unsophisticated approach made it easy for the operators to detect the attack, and there was prior experience in dealing with this situation. In fact, the four servers subject to the attack which were not seriously affected had implemented a load-sharing protocol called Anycast, which was specifically developed to deal with this sort of situation.

This particular attack was not sophisticated (the flood of queries was generated by a fairly sophisticated means, but the queries themselves were simple), and was of limited duration, but it did demonstrate a potential major vulnerability in the operation of the Internet and the global IP-based infrastructure. Further, this is not the first time attackers have probed for vulnerabilities in the DNS hierarchy. Numerous attempts have been made over the last several years by a variety of actors to disrupt DNS operation, including some reasonably sophisticated protocol-based attacks, such as the DNS Amplification Attacks seen in 2006.

A sophisticated adversary could combine the best features of these known techniques and launch an effective attack against the DNS hierarchy, which would certainly degrade Internet operations for whatever period the attacker desired. Further, attacks which rely on surges of traffic to overload machines are easy to detect – although not always easy to deal with. Depending on their intent, the most sophisticated adversaries (who typically don't advertise their presence by causing surges in traffic) could covertly access key computers in the DNS hierarchy, and corrupt the addressing tables. This would be much more difficult to detect: operations would be disrupted, but the cause would not be obvious – and much more difficult to deal with. Address tables could be reloaded from back-up, but the reloaded tables could be immediately corrupted again. An automated tool for implementation of a variation of this approach has recently been announced by security researcher Dan Kaminski. While this announcement caused a flurry of publicity, and trumpeting of some partial solutions such as DNSSEC (a protocol which adds some security authentication to DNS transactions) little of substance has been done to deal with this issue in fundamental fashion.

While the previous discussion focused on the DNS hierarchy, the BGP protocol used for routing packets between Autonomous Systems is also of major concern. There are several widely-recognized vulnerabilities in the protocol itself, and while the IETF is working on a more secure replacement for BGP, implementation is at least several years away. Sophisticated adversaries could use the known BGP vulnerabilities to effectively block the peering points themselves, or cause "black hole-ing" of legitimate traffic.

c. Sophisticated Attacks against End-user Systems and Applications

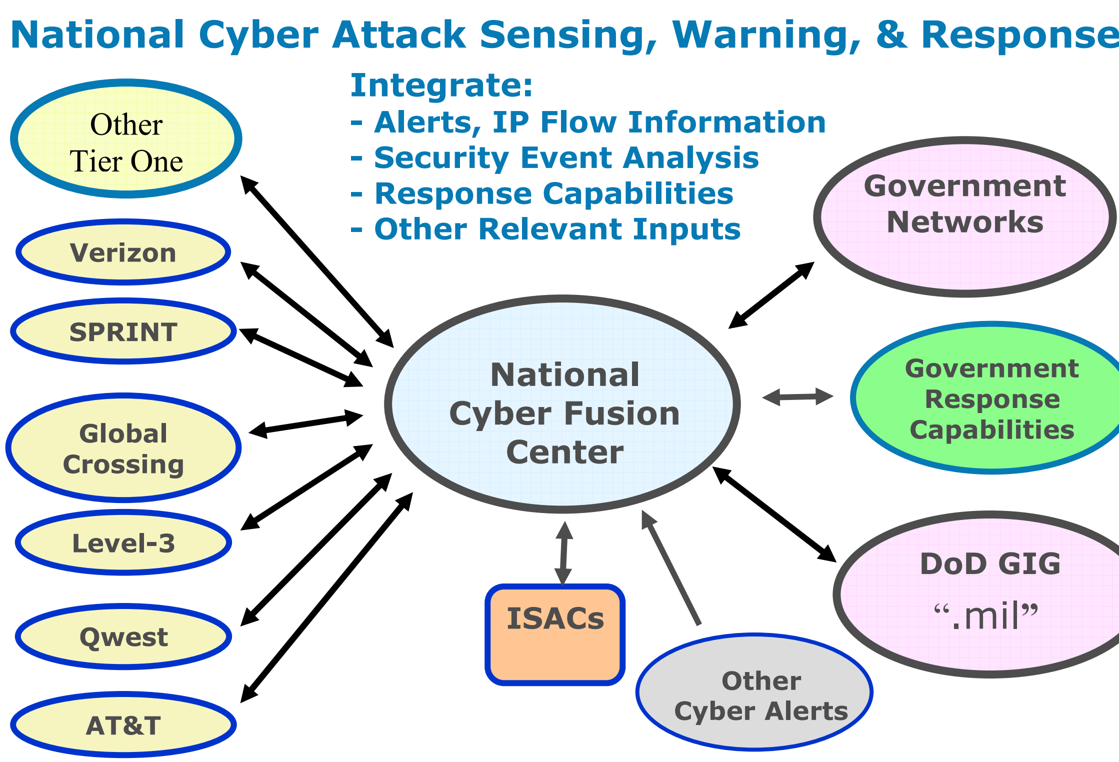
As mentioned earlier, under normal circumstances the sophisticated adversary is not interested in calling attention to their cyber activities. Their objective is to gain access to and control over a computer or system (commonly called a "backdoor") to exfiltrate information of interest, to insert the capability to cause a disruption at some future time, or both – without being discovered. The disruption could take two generic forms: disabling the target computer or system, or corrupting the information. Although these target computers or systems are not a part of the Global Telecommunications Infrastructure per se, the Telecommunications Infrastructure is by far the most convenient vehicle for a sophisticated attacker to accomplish their purpose, so they must be treated together to address the cyber security concerns for protection of the other critical infrastructures.

d. Implications of BotNets

In January 2007, during a panel discussion on the future of the Internet at the World Economic Forum in Davos, Switzerland, Dr. Vinton G. Cerf (currently the Chairman of ICANN, and widely-regard as one of the two founding fathers of the Internet), estimated that approximately one-quarter of the some 600 million computers connected to the Internet had been infected and captured as part of a BotNet. More recent analysis indicates that Dr. Cerf's estimate is conservative, and that the number, size and power of BotNets are increasing rapidly. One BotNet identified by European law enforcement authorities had reached 1.5 million captured computers, and BotNets are now being observed that are implementing defenses against capture of infected computers by other BotNets, and sophisticated techniques to avoid detection. This situation can only be expected to get worse, as computers become more and more powerful, and the number of computers with broadband connectivity continues to expand. One security vendor recently estimated that current BotNets could generate up to 40 Gbps of bogus traffic, more than enough to overwhelm the capacity of the private and public peering points which connect the Global Telecommunications Infrastructure together. .

While most of the currently observed BotNet activity is largely related to criminal purposes, such as Distributed Denial of Service blackmail, SPAM, and identity theft, the implications for the carriers and service providers are clear. An actor who wished to attack carrier networks and systems, and disable or impair their ability to function for a considerable period of time, has the ready means at their disposal. Indeed, a terrorist group or nation state does not have to have a sophisticated knowledge of computers and networks; they only need to recruit or hire one or more of the several thousand BotMasters to do their bidding. A BotNet-based attack with the capabilities known to exist today could simply drown the existing peering points with unwanted traffic, shut down the peering points with BGP attacks, or effectively disable the DNS hierarchy. Any one of these three could isolate the networks of the individual carriers/service providers, and seriously impact the all of our critical infrastructures. A sophisticated adversary could sustain these attacks for an extended period of time, with trace-back to the source extremely difficult or impossible.

Appendix D


National Cyber Attack Sensing, Warning, & Response
Integrate:
- Alerts, IP Flow Information
- Security Event Analysis
- Response Capabilities
- Other Relevant Inputs
Other Tier One
Verizon
SPRINT
Global Crossing
Level-3
Qwest
AT&T
National Cyber Fusion Center
Government Networks
Government Response Capabilities
DoD GIG
".mil"
ISACs
Other Cyber Alerts