THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NETWORK GROUP
INTRUSION DETECTION SUBGROUP
REPORT

Report on the NS/EP Implications of Intrusion Detection Technology Research and Development

December 1997

TABLE OF CONTENTS

Page Number

EXECUTIVE SUMMARY ES-1

1.0 INTRODUCTION 1
- **1.1 Background** 1
- **1.2 Objectives** 3
- **1.3 Scope** 4
- **1.4 Approach** 4
- **1.5 Analysis** 5
- **1.6 Acknowledgments** 5

2.0 ROLE OF INTRUSION DETECTION 5
- **2.1 Definitions** 6
- **2.2 National Risk** 7
- **2.3 Indications, Assessment, and Warning** 10
- **2.4 Intrusion Detection and Network Security Technologies** 11

3.0 INTRUSION DETECTION TECHNOLOGIES 12
- **3.1 Basic Technologies and Functions** 12
  - **3.1.1 Operating Environment** 12
  - **3.1.2 Sources of Information** 13
  - **3.1.3 Subjects Monitored** 14
  - **3.1.4 Technologies and Techniques** 15
- **3.2 Intrusion Detection Systems and R&D Databases** 16
- **3.3 Future Capabilities** 17

4.0 INTRUSION DETECTION END USER REQUIREMENTS 18
- **4.1 General Attributes** 19
- **4.2 Data Management** 20
- **4.3 Detection** 21
- **4.4 Profiling and Pattern Recognition** 22

5.0 ANALYSIS AND FINDINGS 23
- **5.1 National Policy** 23
  - **5.1.1 National R&D Policy Direction** 24
  - **5.1.2 National Response Centers** 25
  - **5.1.3 Basic Research and Applied Development** 25
  - **5.1.4 Global Threats and Local Responses** 26

TABLE OF CONTENTS

5.2 Technology 27
5.2.1 Network Control Elements 28
5.2.2 Scaleable Systems 28
5.2.3 Standards, Testing, and Validation 29
5.2.4 Metrics 30
5.2.5 False Alarms 30
5.2.6 New Attack Profiles 31
5.2.7 Real-Time Alerts 31
5.2.8 Damage Assessment and Response 32
5.3 The Human Element 32
5.3.1 Education, Training, and Awareness 32
5.3.2 Law Enforcement Requirements 33
5.4 Summary of Findings 33

6.0 RECOMMENDATIONS 34
6.1 Promulgate a National Policy to Address Intrusion Detection 34
6.2 Establish an Interagency Working Group for Intrusion Detection 35
6.3 Increase R&D Funding for Control Systems of Critical Infrastructures 36
6.4 Encourage Cooperative Development Programs 36
6.5 Continue to Examine Feasibility of an R&D Consortium 38

Annex A—IDSG Survey Letters

Annex B—Intrusion Detection Subgroup Members and Government Contributors

Annex C—Organizations Contributing to IDSG Efforts

Annex D—Glossary

Annex E—Acronyms

EXECUTIVE SUMMARY

In the past year, the President has demonstrated an interest in protecting the security of the Nation's critical infrastructures. The U.S. information infrastructure is one of the critical infrastructures identified in Executive Order 13010, and it provides services essential to the operation and control of all infrastructures. Assuring the continued operation of the information infrastructure and its key components is a national security priority and business necessity. Increasingly, electronic intrusions represent a threat to the U.S. information infrastructure, and it is clearly in the interest of all parties to bolster the capability to detect those intrusions. Intrusion detection technologies offer promise in terms of combating electronic intrusions, and further research and development (R&D) of those technologies is essential to meeting the collective goals of industry and Government.

The Intrusion Detection Subgroup (IDSG) conducted a study of intrusion detection technology R&D that included: (1) an examination of the role of intrusion detection in the context of indications, assessment, and warning; (2) an overview of existing and planned intrusion detection technology R&D initiatives; and (3) a high-level review of those attributes end users value in their intrusion detection systems. In addition, the subgroup analyzed intrusion detection technology R&D in terms of meeting national security and emergency preparedness (NS/EP) requirements. Specifically, the subgroup identified the following three issue areas requiring attention:

National Policy

The subgroup could not identify a national technology policy that articulated a vision with respect to Federal intrusion detection technology R&D, established Federal research targets and priorities, and coordinated the programmatic efforts of Federal departments and agencies.[1]

Technology

The overarching concern with respect to intrusion detection technologies is that R&D has focused on detecting intrusions in the host or multihost environment rather than at the network and infrastructure levels. The subgroup also identified the need for testbeds and laboratories to develop standards, metrics, and testing procedures that will raise the overall confidence level in intrusion detection systems.

The Human Element

The subgroup determined a need for a Federal investment in educating and training employees on recognizing intrusions and heightening their awareness of the risks associated with electronic intrusions.

---

[1] Over the past 15 months, the President's Commission on Critical Infrastructure Protection has also examined national R&D policy and issued recommendations to the President.

In considering those findings, the Intrusion Detection Subgroup developed the following four recommendations for the President to consider in promoting the R&D of intrusion detection technologies:

Promulgate a National Technology Policy To Address Intrusion Detection

The subgroup recommends promulgating a national technology policy that defines Federal targets and priorities, determines Federal intrusion detection R&D funding levels, and fosters partnerships among Government, industry, and academia. Those activities will raise the national consciousness to the risks associated with electronic intrusions and outline a vision to pursue future R&D opportunities.

Establish an Interagency Working Group for Intrusion Detection

The subgroup recommends establishing an interagency working group to develop Federal R&D targets and priorities and provide program management and oversight. That oversight could include balancing Federal funding levels between basic research and applied development, and identifying emerging technologies and expediting their migration from laboratory to market.

Increase R&D Funding for Control Systems of Critical Infrastructures

The subgroup recommends increasing the R&D funding of technologies that can detect intrusions into the network control and switching systems of the telecommunications infrastructure. In addition, the subgroup recognized the importance of network control elements supporting the operation of other critical infrastructures.

Encourage Cooperative Development Programs

The subgroup recommends the Government encourage cooperative development programs to maximize the use of existing R&D resources in Government, industry, and academia. Specifically, those programs could focus on establishing common standards, metrics, and testing procedures and identifying incentives to foster innovation and increase the pace of technological development.

In addition, the IDSG recommends that the Network Group continue to work closely with the U.S. Government to examine the feasibility of establishing a joint industry-Government R&D consortium focused on network security technologies. This tasking is part of the 1998 Network Group work plan.

1.0 INTRODUCTION

The dependence of all United States government entities, and most notably the Department of Defense (DoD), on commercial telecommunications and computing technologies integral to the U.S. information infrastructure represents a potential vulnerability that threatens the Nation's security. Therefore, assuring the continued operation of the U.S. information infrastructure is vital to sustaining our national and economic security posture. This requirement becomes even more pressing given the pervasive nature of information systems that support the essential operations of the Nation's critical infrastructures. Of particular pertinence is the ability to determine whether those systems are being subjected to acts of electronic intrusion. The continued research and development (R&D) of enhanced technologies to detect intrusions into those systems and to mitigate the effects of successful intrusions are a predominant national security priority and have become a business necessity.

1.1 Background

The President's National Security Telecommunications Advisory Committee (NSTAC) was established in 1982 to advise the President on national security and emergency preparedness (NS/EP) telecommunications and information systems issues. The NSTAC is composed of 30 senior corporate executives (often chief executive officers) from telecommunications, systems integration, and computer companies. The NSTAC principals designate subject matter experts to the NSTAC's subordinate bodies to examine national telecommunications and security issues. A significant part of the NSTAC's mission is to assess the overall security of public networks (PN) and their components.[1] This assessment includes examining emerging threats, evaluating the introduction of new technologies into telecommunications networks, and identifying network vulnerabilities. The result is a characterization of electronic threats and vulnerabilities to telecommunications and information systems.

During the past 2 years, the NSTAC has expanded its efforts by addressing electronic threats to other critical infrastructures. In January 1995, Vice Admiral Mike McConnell, Director of the National Security Agency (NSA), briefed the NSTAC on threats to the U.S. information and other critical infrastructures. The NSTAC principals subsequently sent a letter to the President stating that the Nation's information and other national infrastructures "are increasingly at risk from intrusion and attack."[2] The President replied in July 1995, requesting the "NSTAC's principals-with input from the full range of NII users-to provide me with your

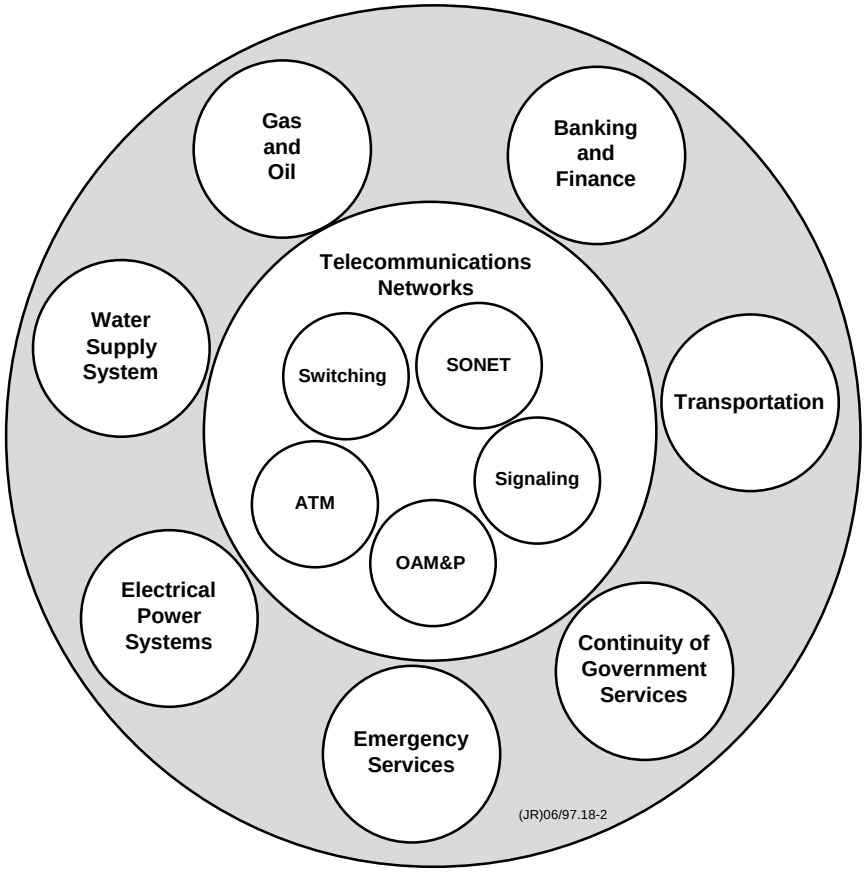
[1] The Network Security Information Exchange has defined public networks as including "any switching system or voice, data, or video transmission system used to provide communications services to the public (e.g., public switched networks, public data networks, private line services, wireless systems, and signaling networks), An Assessment of the Risk to the Security of Public Networks, December 1995, p. ES-2.

[2] Letter from Mr. William Esrey, Sprint Corporation and Chair of the President's NSTAC, to the President of the United States, dated March 20, 1995.

assessment of national security emergency preparedness requirements for our rapidly evolving nformation infrastructure."[3]

The NSTAC's examination of interdependencies among critical infrastructures[4] has underscored the prominent role played by telecommunications and information systems. Specifically, telecommunications and information systems play a critical role in supporting the management and control functions for other infrastructures (Figure 1).

Figure 1
Critical Information Infrastructures



As interdependencies among critical infrastructures proliferate, the need to strengthen network security technologies assumes greater importance. This evolving requirement has been a major impetus for NSTAC action. Specifically, intrusion detection was identified as a critical area requiring further study, and the following activities influenced the establishment of the Intrusion Detection Subgroup (IDSG):

---

[3] Letter from the President of the United States to the NSTAC, dated July 7, 1995.

[4] The NSTAC's Information Assurance Task Force has studied the information assurance risk to the electric power, financial services, and transportation infrastructures.

- The Defense Advanced Research Projects Agency (DARPA) briefed a joint industry-Government meeting on intrusion detection R&D and invited the NSTAC to provide an industry perspective in better focusing those efforts (August 15, 1996).

- The NSTAC's Network Security Group[5] sponsored an R&D Exchange to provide a common understanding of network security problems, identify R&D activities in progress to address those problems, and identify additional network security R&D activities needed. One of the primary discussion topics was intrusion detection technologies (September 18, 1996).

- In response to a request from the Deputy Manager, National Communications System, the NSTAC's Issues Group formed a scoping group to determine possible NSTAC assistance to DARPA in the area of intrusion detection (October 1996).

- That scoping group drafted an issue paper that resulted in the establishment of the IDSG. That subgroup was tasked to provide an industry perspective on intrusion detection R&D activities and to identify related technological, operational, and joint industry-Government issues (November 1996).

1.2 Objectives

The NSTAC tasked the subgroup to consider electronic intrusions into the telecommunications infrastructure and the potential effects of such intrusions on other critical infrastructures. Specifically, the subgroup was charged to perform the following tasks:

- Establish common definitions for *intrusion*, *intrusion detection*, *indications, assessment*, and *warning*.

- Assess current intrusion detection R&D activities and determine if NS/EP considerations require additional effort.

- Coordinate with DARPA, the President's Commission on Critical Infrastructure Protection (PCCIP), and the Infrastructure Protection Task Force (IPTF) to determine to extent to which they were pursuing issues related to intrusion detection research.

- Determine the need for and the benefits of a long-term cooperative industry-Government research effort.[6]

- Develop proposed recommendations to the NSTAC for presentation to the President.

1.3 Scope

[5] The Network Security Group was renamed the Network Group following NSTAC XIX.

[6] The Network Group is planning to address this issue separately.

The IDSG focused on intrusion detection technology R&D, specifically on current intrusion detection R&D activities and broad areas where intrusion detection R&D efforts may require additional funding or direction to address NS/EP concerns. For the purposes of this study, the subgroup concentrated on electronic intrusions into those network control systems that support the telecommunications infrastructure and; through their dependency on information systems; other critical infrastructures. Because other critical infrastructures also rely on similar information systems, intrusion detection technology R&D would have relevance and applicability for them as well. The study did not consider whether intrusions were intentional or unintentional, legal or illegal, or resulted in damage. The subgroup believed that the intent or nature of the attack was not the central issue; rather, the focus of study was the research and development of the technologies required to detect intrusions into systems.

An important element of this study was the role intrusion detection played within the broader context of indications, assessment, and warning (IAW). There is an increasing interest in both subjects at the national level. The subgroup discussed the development of IAW capabilities in its deliberations and considered them to be an essential element of a national strategy to protect the Nation's critical infrastructures. Intrusion detection technologies may play a central role in enabling indications collection and assessment of related data. For this reason, strong intrusion detection tools may be a prerequisite for the development of a strategic IAW capability that examines threats to the Nation. Section 2 discusses this issue in more detail.

1.4 Approach

In response to its tasking, the subgroup took the following actions to collect information on and analyze intrusion detection technology R&D:

- Forwarded a letter to the NSTAC member companies requesting information on their intrusion detection activities

- Forwarded letters to those organizations performing intrusion detection R&D for DARPA that surveyed current intrusion detection R&D projects, their technological focus, and funding sources (Note: Appendix A provides copies of those letters)

- Invited several researchers and vendors of intrusion detection systems (IDS) to present their views to the subgroup

- Interviewed members of the NSTAC Network Security Information Exchange (NSIE). The NSTAC NSIE membership includes network security practitioners from industry who meet bimonthly with their counterparts from Government to share threat and vulnerability information. Those representatives provided the subgroup with their insights into the needs of the telecommunications service providers with respect to intrusion detection.

Subgroup members also participated in technical seminars related to intrusion detection products and R&D activities. They exchanged information with those organizations researching,

developing, or using intrusion detection technologies. These technical seminars included the following:

- DARPA Intrusion Detection Principal Investigators Conference in Savannah, Georgia (February 24-27, 1997)
- National Institute of Standards and Technology (NIST) Practical Intrusion Detection Seminar in Gaithersburg, Maryland (April 23-24, 1997)
- DARPA/Defense Information Systems Agency (DISA)/NSA Information Assurance (IA) Overview Conference in Williamsburg, Virginia (July 9-11, 1997)
- DARPA Intrusion Detection Principal Investigators Conference in Menlo Park, California (July 29-31, 1997).

1.5 Analysis

This study documents the subgroup's findings and recommendations derived from its analysis of information from all noted sources. The subgroup paid special attention to surveying representatives from Government, industry, and academia. In addition, the subgroup received inputs from both the research community and those public and private organizations who relied on intrusion detection technologies to protect their networks from computer intrusions. All data collected from interviews, surveys, and presentations was analyzed on a **nonattribution** basis by the subgroup members and representatives from the National Communications System (NCS). Because the study's scope was limited, some of its findings may be anecdotal in nature.

1.6 Acknowledgments

The subgroup would like to convey its appreciation to those subgroup members, Government representatives, presenters, survey respondents, and other individuals who contributed to the study. Appendix B lists the members and other regular contributors to the subgroup's activities. Appendix C lists those organizations that presented information to the subgroup, responded to the surveys, and NSIE member companies and Government agencies that contributed to the study.

2.0 ROLE OF INTRUSION DETECTION

Examination of electronic intrusions in the context of critical infrastructure protection creates new issues for Government and industry. One issue is how to define new terms of reference related to intrusion detection so that common definitions prevail throughout the entire community. The lack of common definitions can create confusion and in some cases foster mistrust. The IDSG was tasked to develop a common set of definitions for various terms that would be acceptable and understood by all parties. This section defines the key terms in the intrusion detection field and further discusses role of intrusion detection in the context of indications, assessment, and warning.

2.1 Definitions

To aid in examining the technical issues associated with intrusion detection R&D, the IDSG was specifically tasked to develop common definitions for *intrusion, intrusion detection, indications, assessment,* and *warning* that were consistent with and understood by Government, industry, and academia. This was deemed necessary because distinct communities of interest (e.g., defense, intelligence, law enforcement, private sector) often use different terminologies to describe similar concepts. In addition, popular terms of reference from the Cold War are sometimes misapplied to describe emerging cyber threats. Too often, differences in terminology have acted as barriers to dialogue among relevant stakeholders and caused confusion.

An example of this problem is the current description of cyber threats within Government agencies, which even among themselves use different terms to describe identical or related concepts. Some elements of the Defense Department, for instance, refer to *information warfare* and *information warfare-defense* in describing offensive and defensive actions respectively. Other elements of DoD and members of the intelligence community often cite offensive and defensive electronic actions as *information operations*. With elevated concerns in the United States regarding cyber threats, law enforcement and the private sector have expressed concerns about *information assurance*. Although each of these terms has a slightly different meaning or connotation, the reality is that all are focused on the use or potential use of electronic intrusion techniques to exploit, degrade, or deny service to key information systems.

As a result of considering new terms of reference and related issues, the subgroup developed the following common definitions:

- **Intrusion**
  An intrusion is unauthorized access to, and/or activity in, an information system.

- **Intrusion detection**
  The process of identifying that an intrusion has been attempted, is occurring, or has occurred.

- **Indication**
  An indication is information that suggests a threat.[7] Indications include explicit evidence that an intrusion has occurred and implicit evidence revealing the interests, intentions, and capabilities of the threat.
- **Assessment**
  An assessment is the analysis of indications to determine the likelihood, nature, and potential of a threat.

[7] The subgroup defined a threat as "a potential undesirable event, malicious or not, of (1) compromise (i.e., theft of valuable or sensitive information or services), (2) corruption of information or information services, or (3) denial of service by degradation/blocking of data, processing, or communications or an entity possessing the capability and intent to cause the above."

- **Warning**
  A warning is an advisory of the results of the assessment, likely targets, and recommended actions.

These definitions are consistent with those already being used by Government, industry, and academia. The subgroup hopes that common definitions will assist in stimulating a general dialogue among stakeholders.

2.2 National Risk

The prospect of cyber attacks against the U.S. information and other critical infrastructures has generated a great deal of interest within the Federal Government and the private sector. Recent activities reflect this intensified level of national interest:

- **The Kyl Amendment**
  This amendment to the National Defense Authorization Act for Fiscal Year 1996 required the President to report on policies leading to the development of a national architecture for an indications, warning, and assessment capability focused on strategic attacks against the U.S. information infrastructure.

- **Security in Cyberspace Hearings**
  The U.S. Senate Permanent Subcommittee on Investigations conducted hearings during summer 1996 to examine growing threats to U.S. defense and commercial systems. The resultant minority staff report discussed actions to improve the Nation's preparedness against international threats.

- **Executive Order 13010**
  President Clinton signed Executive Order 13010, *Critical Infrastructure Protection*, July 15, 1996, establishing the PCCIP and IPTF. These organizations are responsible for analyzing cyber and physical threats to eight critical national infrastructures.[8]

- **Defense Science Board Report on Information Warfare-Defense**
  The Defense Science Board Task Force on Information Warfare Defense was established to examine the Nation's information dependency and issued 13 high-level recommendations to improve the Nation's defense posture with respect to information warfare.

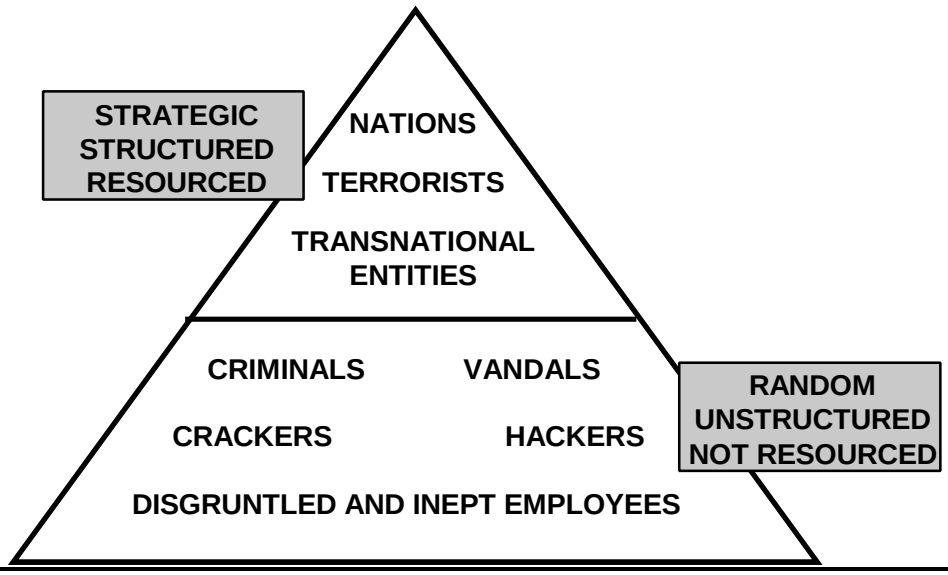
In each of these initiatives, the national security and economic security dimensions of cyber threats were explored. In the *Security In Cyberspace* hearings, for example, significant evidence was presented characterizing defense systems as increasingly vulnerable to network intrusions and probing. The General Accounting Office (GAO) presented its study of intrusions

[8] Executive Order 13010 designates eight critical infrastructures: information and communications; electric power systems; gas and oil transportation and storage; banking and finance; transportation; water supply systems; emergency services; and government services.

into DoD systems[9] and explained the high costs associated with intrusions in terms of staff demands and the effects of computer downtime. The hearings also focused on the importance of the Nation's infrastructures; information and communications, electric power, finance and banking, and transportation; and how risks to them could significantly affect our economic strength and national competitiveness.

The linkage between national and economic security offer a common ground for Government and industry. Both require a reliable and robust infrastructure to meet their varied needs. The military, for instance, needs a robust and reliable transportation infrastructure to deploy and sustain forces overseas. Similarly, the financial services and electric power infrastructures depend on the reliability and availability of telecommunications to transmit automated transactions, manage the operation of their networks, and conduct electronic commerce. Although infrastructure failures could be catastrophic from a national security perspective, it is equally relevant to indicate that those same failures and outages would also have profound implications for businesses. Furthermore, as Government increasingly relies on the private sector and its assets, failures in commercial infrastructures could seriously affect its ability to meet its NS/EP requirements. In its examination of information-based risks to other infrastructures, the NSTAC developed Figure 2 to describe threats.

Figure 2
The Threat Pyramid



The pyramid depicts different levels of threat. At the top of the pyramid are those organizations with the capability, resources, and intent to orchestrate strategic attacks against the United States and its infrastructures. It is generally assumed that, in the current context, the number of structured and resourced threats to mount a *strategic* attack is relatively small. The

9 Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, General Accounting Office, May 22, 1996.

threats depicted lower on the pyramid are more common but less resourced and coordinated. Although unstructured attacks may occur more regularly, they appear to present a limited strategic threat to national and economic security interests.

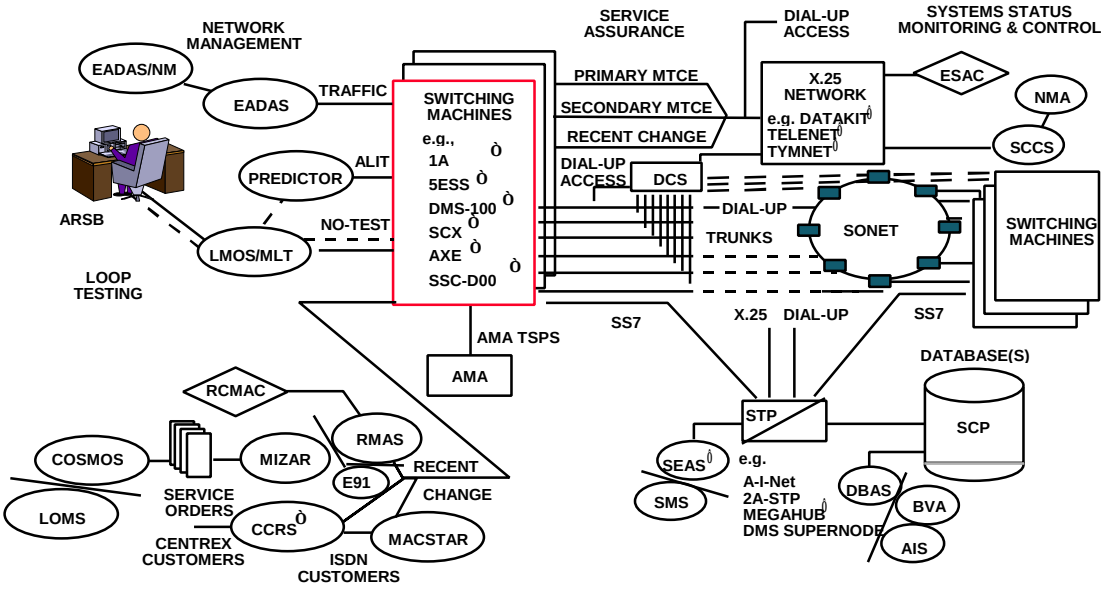
Companies have instituted organizational responses to the threats depicted at the lowest end of the pyramid. Systems administrators and security professionals encounter these types of threats regularly and recognize their potential implications in terms of revenue lost or network downtime. In general, these threats occur at a localized level. However, the more sophisticated and structured threats may occur across networks and infrastructures, and could be driven by national and economic security considerations. Response to a foreign power or state-sponsored group using cyber techniques against numerous companies requires coordination across Government agencies and across privately owned and operated infrastructures.

Insiders may participate at any point depicted in the pyramid. The Office of the Manager, NCS (OMNCS) has defined insiders as "legitimate users of computer systems who use their knowledge of that system to circumvent computer security protection measures."[10] Insider attacks can affect all components of a computer system. Because of their knowledge of the computer system, an organization's computer security practices, and plausible access requirements, insider attacks can be perpetrated with little personal risk. Nation-states, terrorists, or organized crime entities may "plant" insiders to achieve their objectives, or may compromise the integrity of insiders through extortion, threats, or bribery. Insiders also may participate in an organized hacker activity or act independently for profit or revenge.

Regardless of the nature of the threat, several key components of the telecommunications infrastructure are more critical than others. Figure 3 depicts the key components of a public network, including the operations, administrative, maintenance, and provisioning (OAM&P) system, signaling , switching, network management, and transmission systems that may be at risk to electronic intrusion.

10 The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document, Office of the Manager, National Communications System, September 1994.

Figure 3
PSN Risk Analysis Environment



Source: Bellcore

Those components represent the "crown jewels" of public networks. Interruption in their operation could have significant service and financial implications for specific companies and (depending on the scope of an attack) possibly infrastructure-wide implications. In addition, threats to control networks are not limited to the telecommunications infrastructure. As other critical infrastructures seek to exploit information technologies and migrate to more open systems, their control networks may be similarly exposed.

2.3 Indications, Assessment, and Warning

Development of a strategic IAW capability is one method identified to better protect infrastructures from attack. In responding to cyber attacks, just as in the nuclear and terrorist arenas, the indications and warning process involves a wide range of data and information gathering, fusion, and analysis capabilities leading toward identification of specific impending harmful effects. Intrusion detection systems are likely to be an important component in sensing indicators.

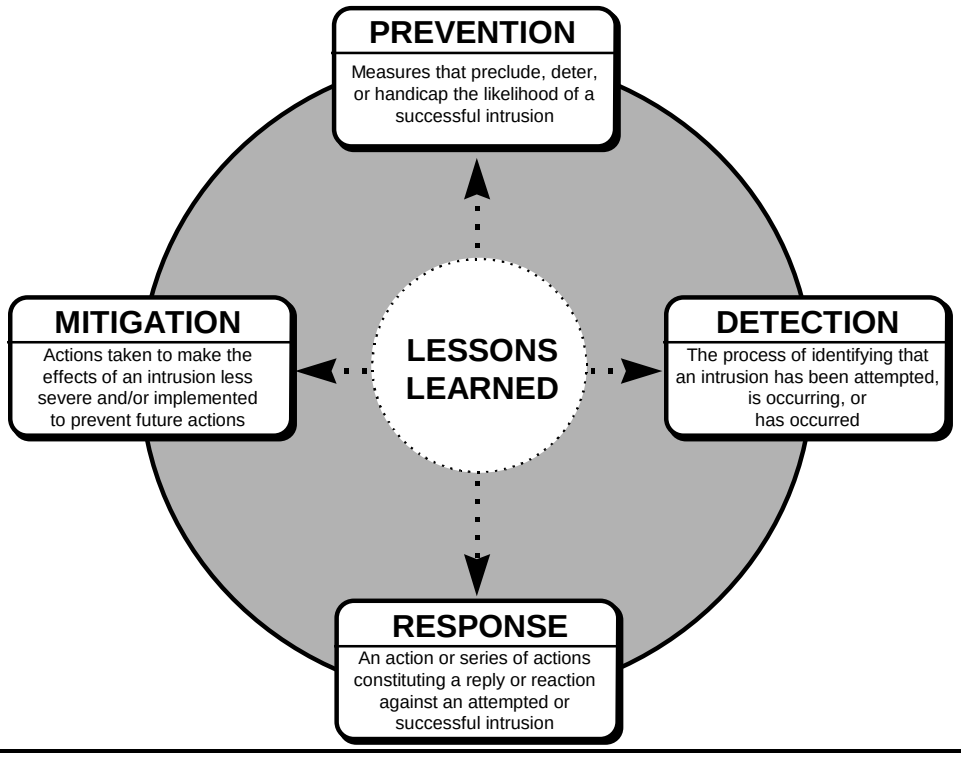
For the purposes of developing indications and warning for cyber attacks, sensors must provide confidence levels appropriate to their use and their confidence levels must be known so that the analysis of detected intrusions can be properly reflected in the indications and warning process. A strategic IAW capability for cyber attacks must reliably differentiate events so that false negatives and false positives¢ prominent in today's environment¢ do not lead to missed or false warnings. Although the overall cyber attack indications and warnings process is important,

this report concentrates only on the intrusion detection issue. Other aspects of cyber attack indications and warnings are beyond the scope of this report and will not be considered further.[11]

2.4 Intrusion Detection and Network Security Technologies

Intrusion detection technologies are promising because they may offer indications that can be analyzed to produce an assessment of the overall threat. Although the remainder of this report focuses on intrusion detection technologies, the subgroup also wanted to acknowledge the importance of three other elements that constitute a robust network security strategy: prevention, response, and mitigation. Figure 4 is a notional depiction of those four elements. *Prevention* measures preclude, deter, or handicap the likelihood of a successful intrusion. An example of a preventative measure is a firewall, which may preclude unauthorized users from accessing the network. *Response* is an action or series of actions constituting a reply or reaction against an attempted or successful intrusion. Finally, *mitigation* includes actions taken to make the effects of an intrusion less severe or harmful and/or actions implemented to prevent future actions. Those three elements, when combined with intrusion detection, constitute a process by which the lessons learned from any single event can be input to each respective element to improve the overall security of a networked system.

Figure 4
Four Elements of Network Security



[11] The NSTAC is examining the policy and operational dimensions of IAW in its National Coordinating Center for Telecommunications Vision Subgroup.

3.0 INTRUSION DETECTION TECHNOLOGIES

This section reviews current state-of-the-art intrusion detection technologies, including basic intrusion detection technologies and techniques; sources of information regarding fielded intrusion detection systems; and an overview of future capabilities and technologies being researched to improve intrusion detection systems. The primary sources of information for this section were:

- **IDSG Survey Letters**
  The subgroup analyzed the 20 responses to its survey letter from industry, academia, and Government organizations. (Those organizations providing submissions are summarized in Appendix C.)

- **Principal Investigators Conferences**
  Representatives from the subgroup interacted with the research community at the February 24-27, 1997 (Savannah, Georgia) and July 29-31, 1997 (Menlo Park, California) DARPA Principal Investigators conferences.

- **Direct Research from Literature and the Internet**
  The subgroup reviewed numerous technical reports on intrusion detection technology and visited sites on the World Wide Web with information on intrusion detection technology (Section 3.2 provides a partial listing of those WWW sites).

3.1 Basic Technologies and Functions

Effective detection technologies and techniques are key to managing the risks associated with unauthorized intrusions. Intrusion detection systems operate within four contexts: operating environment, sources of information, subjects monitored, and technologies and techniques being employed in fielded systems. Each of these are described as follows.

3.1.1 Operating Environment

The standard operating environment has evolved over time from being strictly host-based to include networked systems. Intrusion detection systems operate within several different operating environments, which are summarized as follows:

- **Host-Based Environment**
  All the audit data processed by the intrusion detection system is derived from activity on a host processor. The intrusion detection system does not look beyond user, application, and system data generated on the host to network-based data.

- **Multihost Environment**
  This remains a host-based environment, but audit data from multiple hosts is collected and used to detect intrusions. Note: the hosts in a multihost environment may or may not be interconnected.

- **Networked Environment**
  The intrusion detection system looks beyond the data available from host-based activity to incorporate network traffic data. Host data and network data are assimilated to detect intrusions.

- **Infrastructure Environment**
  This environment evolved from individual stand alone information processing systems to enterprise-wide and industry-wide systems. An infrastructure is a common communications medium used by many independent but related organizations.

3.1.2 Sources of Information

Intrusion detection systems collect and analyze information from many sources, but most of the data gathered are from user, application, system, and network state activity. Intrusion detection systems also can process raw input data. Data also may be entered manually into intrusion detection systems for processing. The following lists some data sources available to intrusion detection systems:

- **System Logs**
  System logs capture process and system activity (e.g., process start, stop and run times, resource use, system starts and restarts).

- **Audit Logs**
  Audit logs capture user activity (e.g., login activity, file accesses, commands run).

- **Application Logs**
  Application logs reflect the run-time characteristics of the application (e.g., runs continuously, periodically, or on demand; may or may not require human interaction).

- **Network Management Logs**
  Network management logs ensure control and configuration activities are issued to the network devices. These logs provide device health and status information and record device state transitions.

- **Network Traffic Capture**
  Network traffic captures use sniffers to capture data packets traveling across the network. Packet headers provide source and destination information for analysis. Data content can be scanned for key text strings.

- **Manual Entry**
  Manual entry uses rules to determine the way in which raw data is evaluated. Lists of key search items or users can be developed and updated or deleted from as new information warrants.

- **Derived Data**
  Derived data ensures that intermediate results derived from raw input data are made available for follow-on processing. Derived data may result from numerical or logical computations.

3.1.3 Subjects Monitored

The subject or focus of intrusion detection system activity continues to change, partly in response to the evolution of computer systems from isolated stand alone systems to large-scale, widely distributed, highly interconnected systems. The change in focus also arises in response to the need to increase an organization's understanding of the intrusion detection process. The following is a partial list of intrusion detection monitoring subjects:

- **Users**
  Initially, intrusion detection was human-oriented in that the discipline was focused on individual users and their actions.

- **Groups**
  Groups are an aggregate form of the user focus.

- **Systems**
  Systems are composed of more than human users. They include hardware devices, software device drivers and handlers, libraries, resource management software, scheduling software, etc. These elements also can provide indicators of an intrusion.

- **Applications**
  Where it might be infeasible to monitor thousands of individual users of a specific application, much can be learned by focusing on the application itself. Because most applications behave in a well-defined manner, deviations from their normal operating patterns may indicate an intrusion.

- **Networks**
  Networks can provide indications of intrusions. For example, network traffic analysis can develop a profile of what is normal for a given network. Data packet analysis can determine a normal set of source and destination Internet Protocol addresses.

- **Interfaces**
  If two systems communicate and share specific data regularly, it is possible to develop a profile of the interface (e.g., the data exchanged, how often, the volume, senders, recipients).

3.1.4 Technologies and Techniques

System administrators employ basic technologies and techniques to detect intrusions, some of which are explained below:

- **Data Collection, Reduction, and Analysis**
  All intrusion detection capabilities are based on having a flow of the appropriate data from as many sources as required to determine that an intrusion is occurring or has occurred. In most intrusion detection systems, the data is automatically collected and reduced, but the analysis remains manual.

- **Profiling**
  Profiling techniques analyze the data collected and presented to an IDS to determine "normal" behavior for a user, application, or system. Significant deviations from the norm, referred to as anomalous behavior, are flagged as potential intrusions.

- **Expert Systems**
  Expert systems, which are driven from an encoded rule base, can be used to monitor policy compliance (e.g., a rule might be developed that monitors for attempts to alter database access controls by anyone other than the database administrator). The rules can be as simple as discrete events or as complex as applying the logical AND/ORing to multiple pieces of data. The expert system does not try to differentiate normal from anomalous activity. Rather, it applies the rules individually or in combination to ensure that all users are within their privileged rights.

- **Monitors**
  System monitors function passively, continually analyzing the data presented to them. System monitors are very similar to antivirus functions in that they can detect what has been defined to them. Monitors can detect trends over time. Examples of monitoring systems include event recognition, pattern or signature recognition, trend analysis, threshold checking, and boundary checking.

- **Scanners**
  Scanners represent a philosophical change in the approach to intrusion detection. Unlike other intrusion detection tools that report when a threshold has been exceeded, scanners can be more proactive in seeking security holes, known vulnerabilities, and unauthorized hardware and software. They also seek more subtle clues that could indicate intrusions by checking file integrity, policy compliance, and code changes.

- **Reporting**
  When a suspected intrusion is detected, it must be brought to the attention of the appropriate personnel to assess the indications. Reporting can be periodic printed reports of event information based on a timing mechanism or asynchronous alerts issued based on a defined event trigger. Reporting mechanisms include printed reports, e-mail alerts, audible alerts, and graphical displays.

- **Response**
  If, as a result of the assessment activity, an electronic event is determined to be an intrusion, the next step is to define and initiate the appropriate response actions.

Response capabilities generally are in one of two categories: engage (i.e., active pursuit to learn, discipline, or prosecute) or disengage (e.g., disable account, disconnect communication link). Policy is the key driver of response choice. If the choice is to engage with the intention of taking legal action, special attention must be given to data capture,[12] protection, and integrity. Personnel engaged in this process must know what constitutes "evidence" for a prosecution and how to handle that evidence properly.

3.2 Intrusion Detection Systems and R&D Databases

There are dozens of sites on the World Wide Web that maintain lists of commercially available intrusion detection products, noncommercial systems, and current or planned R&D projects. It was not the purpose of this study to evaluate specific intrusion detection products or research projects. However, the following section lists some Internet sites that detail widely used intrusion detection systems and products and provide links to promising research projects:

- **COAST site at Purdue University**
  (http://www.cs.purdue.edu/coast/ids/ids-body.html)

- **Michael Sobirey site**
  (http://www-rnks.informatik.tu-cottbus.de/~sobirey/ids.html)

- **SRI International site**
  (http://www.CSL.sri.com/intrusion.html)

- **University of California-Davis site**
  (http://seclab.cs.ucdavis.edu/projects.html)

- **Lawrence Livermore National Laboratory site**
  (http://doe-is.llnl.gov/nitb/docs/nitb.html)

- **An Introduction to Intrusion Detection**
  (http://www.techmanager.com/nov96/intrus.html)

- **Computer Incidence Advisory Capability**
  (http://ciac.llnl.gov/cstc/nid/niddes.html)

3.3 Future Capabilities

Responses to the IDSG survey letter identified several areas of intrusion detection research as being increasingly important in terms of priority and funding. These broad areas include intrusion detection systems with the following characteristics:

- **Operate on an Interdomain Level**

[12] Capture and retention of information are governed by U.S. and international law.

Initial research is being conducted into those intrusion detection capabilities that can operate between physically distinct network domains and logically distinct organizational domains.

- **Mimic the Human Immune System**
  There are research projects focused on detecting intrusions modeled after the human immune system and its ability to fight "infections." This approach could offer systematic detection and repair.

- **Address Network Control and Switching**
  Early efforts are underway to develop systems that can detect and assess intrusions into network control and switching technologies (i.e., Signaling System 7, broadband ISDN, and supervisory control and data acquisition systems).

- **Recognize Unknown Attack Patterns**
  Research projects are concentrating on developing systems to recognize heretofore unknown attack scripts and patterns being used by electronic intruders.

- **Anticipate or Predict Attacks**
  Research efforts are attempting to develop "proactive" or "predictive" systems, sensors, and techniques to anticipate attacks based on preliminary indications. Such systems and techniques require both interpolation and extrapolation.

- **Assess Damage**
  Some research projects are focusing on the development of systems that can contain and assess damage and identify measures to assist network recovery.

- **Function as Agents**
  Software agents are being used to address data collection in today's distributed, heterogeneous environments. Research examining the use of cooperating autonomous agents is being conducted. These agents are tailored to the environment in which they are deployed.

- **Employ Wrappers**
  Wrappers are a technique aimed at addressing the issues of legacy systems and heterogeneous environments. When it is infeasible to upgrade the system (software or hardware), new modules (software or hardware) can be placed at the system access points to monitor, control, and collect data as information flows into and out of the system. Wrappers can be developed that act as front ends for a wide variety of systems.

- **Use Embedded Software**
  Partly in response to the distributed design of current computer systems and in recognition of the fact that certain critical devices control data flow throughout these systems, some researchers are examining the use of embedded software. This

software could have security features embedded in its design to recognize and respond to network intrusions.

In addition, the following advanced methods and techniques are being investigated by the intrusion detection research community:

- Cooperating detectors
- Statistical anomaly detection
- Machine learning
- Meta-learning
- Computational immunology
- Quantitative evaluation of effectiveness
- Model-based detection
- Graphical detection
- Specification-based detection
- Thumbprint technique
- Software agents for intrusion detection
- Network and system instrumentation
- Network monitoring
- Signaling infrastructure detection
- Detection in high-speed networks
- Automated response
- Survivable active networks
- Planning and procedural reasoning.

4.0 INTRUSION DETECTION END USER REQUIREMENTS

This section analyzes responses from end user communities (both public and private) regarding their current and anticipated requirements with respect to intrusion detection systems (IDSs). **For the purposes of this study, the IDSG defined end users as those individuals responsible for operating, managing, and administering networked systems.** Those individuals include systems administrators, security professionals, and network administrators and managers. This section outlines the general attributes identified by those end users as being requirements in IDS and describes additional IDS functions in the area of data management, detection, and profiling. Information for this section was derived from:

- **NSTAC Member Companies**
  The subgroup discussed intrusion detection issues with representatives from the NSTAC member companies.

- **Network Security Information Exchange**
  The subgroup met with representatives from the NSIE to determine their perspectives on intrusion detection technologies.

- **Principal Investigators Conferences**

The subgroup interacted with end users at the DARPA Principal Investigators conferences.

- **Intrusion Detection System Vendors**
  The subgroup received numerous presentations from vendors of intrusion detection systems.

4.1 General Attributes

End users identified the following attributes as essential to manage risks to their systems:

- **Scalable**
  As systems become more complex and interconnected, end users will require IDSs that can be scaled to detect intrusions across different networks, platforms, and applications.

- **Interoperable**
  Due to the heterogeneity in the software and hardware of today's distributed and interconnected systems, end users require IDSs that can interoperate with a diverse set of operating systems, platforms, and applications.

- **Automated**
  In the massively complex and heterogeneous networks of today, manual review of audit and alert logs is an increasingly difficult (if not impossible) task. End users require systems that use automated features to assist them in identifying potential or actual intrusions and fusing the data for analysis.

- **Integrated**
  As noted previously, organizations are using different operating environments, systems, platforms, and applications to meet their changing needs. End users will increasingly require IDSs that have features and functions that can be easily integrated with those of existing network management tools.

- **Affordable**
  Despite an emphasis on IDSs, organizations have generally devoted limited budgets and human resources to managing the risks associated with security concerns. Users will require IDSs that reflect the budgetary realities that system administrators and security professionals operate within.

- **Adaptable**
  Information systems and networks are upgraded regularly to keep pace with technological advances. End users will require IDSs that offer configuration options that can be tailored to their unique operating environments to provide global solutions for networks.

- **Easy to Use**
  End users have a wide range of responsibilities. To avoid unnecessary expenses in terms of training while keeping pace with technology, users will require user-friendly IDSs that provide "point and click" solutions to detecting intrusions.

- **Verifiable**
  End users need the capability to test, verify, and evaluate the accuracy of IDSs. To provide measures of effectiveness and other metrics, end users will require testing and validation procedures in both the laboratory environment and in the field to verify the capabilities and performance of IDSs.

4.2 Data Management

System administrators have a wide range of responsibilities and a limited amount of time and resources to devote to security. Time and resource constraints often limit the ability of system administrators to analyze the great quantities of audit and alert information generated by their network management and intrusion detection systems. To meet their security needs, system administrators require IDSs that are automated, seamless, and capable of reducing and analyzing vast amounts of information. From a data management perspective, the following requirements were identified:

- **Acceptable Impact on the Operating Environment**
  Networking technologies are being used to improve productivity, efficiency, and competitive advantage. Organizations place a premium on accessibility and, consequently, IDSs will need to be transparent to all users of the network.

- **Adaptable to New Environments**
  As noted above, operating systems are upgraded regularly to keep pace with technological advances. For example, some organizations are migrating to Windows NT or other new operating systems. The result is systems are more technologically complex, open, distributed, and heterogeneous. This will require IDSs that can adapt to new operating environments while maintaining base functionality.

- **Bundle Solutions**
  Organizations manage networks composed of diverse hardware and software products purchased from different vendors to meet their network management and security requirements. Users expressed a concern about having IDSs that could be easily integrated with existing network management capabilities. IDSs should be interoperable so they can be bundled to function in heterogeneous environments. Further, they must be bundled in a manner to present a "single face" to end users.

- **Responsive to Cost Versus Performance**
  In the current business environment, organizations are streamlining their business processes to maximize performance. Like other managers, system administrators and security managers are required to justify the costs of security technologies against their

potential performance and impact on the bottom-line. Those costs are often justified in the context of risk management. However, current IDSs do not provide good measures of performance that quantify the cost savings to the organization based on detected intrusions.

- **Easily Tested and Evaluated**
  As noted previously, organizations have increased pressures to quantify their returns on investment. Testing and validation procedures provide organizations with a method to determine effectiveness and differentiate between products. Currently, there are no standard test procedures, standard test case scenarios, or certification processes to provide organizations with appropriate guidance in terms of cost and performance.

An additional concern the subgroup identified was developing intrusion detection capabilities that are responsive to the needs of the law enforcement community. Collecting information and protecting the chain of evidence of computer intrusions so that it will stand up in court has always been a challenge for system administrators and law enforcement.

4.3 Detection

There is an increasing emphasis on detecting intrusions as quickly as possible to minimize damage and to avoid financial loss, exploitation, or denial of service. To meet the challenges presented by electronic intrusions, system administrators require access to real-time and robust IDSs. Specifically, users identified the following requirements:

- **Function in Real-Time**
  Electronic intrusions can quickly result in financial losses, theft of intellectual property, or other damage. Users require systems that function in real-time or near real-time to allow organizations to respond promptly to mitigate the effects of the attack and assess damage.

- **Perform Autonomous Actions**
  The sheer complexity of large-scale information systems requires a significant analysis of network traffic to ascertain and analyze patterns of normal and anomalous system behavior. IDSs must detect suspicious actions, determine the source, and institute autonomous responses.

- **Perform Coordinated Actions**
  Organizations use a variety of techniques and products to protect their networks. Users require IDSs that are flexible enough to interface with other security and network systems and products. The activity of one intrusion detection component may, for instance, be viewed as suspicious by another intrusion detection component if they are not properly configured and coordinated. The result could be disruptive false positive alarms.

- **Maintain Low False Alarm Rates**
  To ensure full effectiveness and use, organizations must have confidence in their protections. A high rate of false alarms may erode an organization's trust in the system. Current IDSs have significant problems with returning false positive and false negative alerts. False positives occur when IDSs detect and identify an event as an intrusion when in fact no intrusion has occurred. There may be, for example, network tools used by systems administrators that initiate actions that appear anomalous to an IDSs. In response, an alarm might be issued, diverting the attention and time of the systems administrator and security staff. False negatives are instances where IDSs fail to detect an intrusion while it is occurring or after it has occurred. The result could be a slow response to the intrusion that might result in financial loss, network damage, or some other form of exploitation.

4.4 Profiling and Pattern Recognition

There is a need to address the difficult problem of tracking the wrongful activities (e.g., abuse, misuse, unauthorized access) of insiders, curious, unknowing, or rogue users who are in a position to cause harm. Profiling allows system administrators and security professionals to detect anomalous behavior to identify, discipline, and prosecute intruders. Pattern recognition allows system administrators and security professionals to identify attack signatures and patterns to ascertain methods employed. To develop better profiling techniques, IDSs require more automated collection and analysis tools that can assist the system administrator or security professional in determining the extent of the intrusion. Specifically, the following requirements were identified:

- **Dynamic Systems that Respond to New Attacks**
  Hackers, criminals, insiders, and other intruders are continually upgrading their attack tools, techniques, and methodologies. As new techniques are employed against networks, users will want IDSs that match this increased level of sophistication.

- **Automated Systems that Discern Patterns**
  As intruders diversify their electronic techniques and tools, IDSs will need to collect, analyze, compile, and decipher attack profiles, patterns, and scripts. This process provides the system administrator with an idea of what he or she is confronting and may indicate which vulnerability is being exploited and suggest the most appropriate countermeasures.
- **Cross-Platform Profiling.** Intruders often use identical techniques against different companies and networks. System-to-system interfaces that compile attack scenarios or patterns will enable systems administrators to detect attacks across network nodes.

5.0 ANALYSIS AND FINDINGS

This section describes the analysis and findings of the Intrusion Detection Subgroup based on its study of intrusion detection technologies and current or planned R&D initiatives. Although

numerous studies of intrusion detection systems and technologies[13] have already been conducted, this study focused on identifying methods to influence intrusion detection technology R&D so that NS/EP requirements can be satisfied. In analyzing the NS/EP dimensions of intrusion detection technology R&D, the subgroup identified three levels of concern:

- National Policy
- Technology
- The Human Element.

The findings of this study and related efforts demonstrate the increasing importance of intrusion detection and reinforce the need to address the following issues.

5.1 National Policy

For more than 50 years, the Federal Government has played a central role in funding and directing the Nation's R&D efforts. Robust Government support to R&D programs was perceived as a primary way to ensure the United States retained access to the "best" technologies available to meet its national security objectives. Throughout the Cold War, the Government managed a national R&D effort to fund military programs, national laboratories, private companies, and university research programs. The application of the combined expertise and resources of those entities resulted in the development of leading-edge technologies that enabled the United States to deter the Soviet threat during the Cold War, lead the world in space exploration, and market new "spin-off" products.

In today's competitive environment, R&D investments are increasingly driven by market imperatives**S**high probability of payoff, commercial viability, and rapid prototyping from the laboratory to marketplace. Because national security and defense programs represent a shrinking market, industry is not willing or able to spend its limited R&D funds on high-risk and limited use technologies. The Government remains the only entity with the resources to invest in those high-risk R&D initiatives. Many of those efforts have no guaranteed payoff or defined commercial application. For this reason, shortfalls in Government policy, funding, or direction can have a significant impact on the future research, development, and growth of specific technologies and, indirectly, entire industries. As such, failures on the part of Government, industry, and academia to work together can create disconnects between what technologies are being researched and those being used in the commercial marketplace.

5.1.1 National R&D Policy Direction

The Government has expressed increasing interest in protecting the security of the Nation's critical infrastructures. As evidenced by the establishment of the President's Commission on Critical Infrastructure Protection, the President has identified the need to protect

[13] In particular, the subgroup would like to refer readers to the National Technical Baseline Intrusion Detection and Response Report developed by Lawrence Livermore National Laboratory and Sandia National Laboratories. In many respects, the findings of this study corroborate those outlined in that report.

those infrastructures from physical and cyber attacks. The Commission has considered national R&D policy in its analysis of physical and cyber threats to the Nation's critical infrastructures, and has issued a report to the President recommending an increase in R&D spending. Additionally, there has been a concerted effort within the Defense Department and intelligence community to address the threats posed by information warfare. Targeted IW attacks against military systems (e.g., command & control, communications, intelligence, logistics) have the potential to disrupt the deployment and sustainment of U.S. forces abroad in times of national emergency. An even greater problem is the difficulty associated with addressing the extent of the Government's role, if any, in protecting those commercially owned and operated infrastructures.

The subgroup identified multiple Federal departments and agencies providing funding to research institutions in the area of intrusion detection technology.[14] However, despite national level concerns about electronic intrusion threats, the subgroup was unable to identify a national policy directing and coordinating national R&D efforts to develop the next generation of intrusion detection systems and technologies (or other network security technologies for that matter). Specifically, the subgroup found that:

- There is no national policy promulgating a Federal R&D strategy or vision with respect to intrusion detection that articulates objectives, targets, and priorities.

- There is no Federal department, agency, or interagency working group responsible for managing and overseeing Federal intrusion detection R&D programs, establishing appropriate funding levels, and preventing duplication of effort. This can result in a fragmented and uncoordinated approach to intrusion detection R&D.

- There appear to be no formal processes or structures to identify and champion emerging and commercially viable intrusion detection technologies and move them from the laboratory to the marketplace in an expedient manner.

- There appears to be only minimal coordination between industry, Government, and academia with respect to fostering the development of next generation intrusion detection technologies. And there is little or no emphasis at the Federal level, in particular, on developing programs and incentives to foster competition, increase the pace of development, and encourage innovative solutions from industry.

5.1.2 National Response Centers

Closely related to the above issue is the Government's efforts to develop incident response capabilities to electronic intrusions. The subgroup discerned a noticeable trend within Government spending to concentrate on spending large amounts of money to build and staff IAW/command & control centers. In completing its study, the subgroup identified several

[14] The subgroup identified the following Government sources of R&D funding in the area of intrusion detection technology: Defense Advanced Research Projects Agency, Defense Information Systems Agency, National Security Agency, National Institute of Standards and Technology, and Department of Energy.

organizations interested in or actively establishing operational centers to collect intrusion information, decipher indicators, assess potential threats, and issue alerts. For example, the Defense Information Systems Agency, the National Security Agency, and the Federal Bureau of Investigation have invested significant resources to establish their own operational centers capable of performing some or all of the above functions. In some, but not all, cases, those centers would issue alert notifications to the owners and operators of critical infrastructures.

Although the desire to establish IAW/command and control centers is understandable, such efforts are diverting needed resources away from other elements of a more comprehensive strategy to combat electronic intruders. Having established capabilities to respond to electronic intrusions is essential, but it is equally important to research and develop prevention and detection technologies that permit all end users to develop a more robust and well-rounded capability to protect their networks. Specifically, the subgroup found that:

- A disproportionate share of Federal resources are being devoted to addressing electronic intrusions through the establishment and staffing of IAW/command & control centers rather than on developing better intrusion detection technologies and prevention schemes that could be applied in the public and private sectors.

5.1.3 Basic Research and Applied Development

In analyzing responses to the survey letter and in discussing intrusion detection technologies with vendors and end users, it was clear to the subgroup members that a large portion of available Federal funding was being funneled toward basic research opportunities. Federal programs sponsored by DAPRA, for instance, appeared to focus on providing seed money to research institutions to fund basic research programs. Generally, basic research is a very "hit or miss" process, individual projects are awarded grants to pursue narrowly focused research for specific technologies. Although some tremendous advances may occur through the findings of one of those projects, others will never reach the point of attaining commercial viability.

If commercial vendors and end users are to reap the rewards of today's basic research in intrusion detection, technologies that offer the most promise must be identified, championed, and fast-tracked in terms of funding and testing. For instance, experimental applications or technologies may exist today in the laboratory that could prove useful in detecting intrusions. In the current environment, however, it is unclear how emerging technologies would be identified and championed to ensure they progressed from the laboratory to the marketplace. Specifically, the subgroup found that:

- A disproportionate share of Federal funding is being devoted to basic research while applied development of existing technologies does not appear to be a priority. There may be technologies in existence today that can, if properly applied and tested, provide commercially viable solutions to electronic intrusions. The key is identifying the most promising technologies and ensuring they progress from the laboratory to the marketplace as quickly as possible.

- No formal processes and structures are in place to identify and champion emerging technologies in the basic research arena and move them into applied development.

5.1.4 Global Threats and Local Responses

Individuals, groups, or nation-states interested in using electronic intrusion techniques have access to an increasing number of hacker tools. As the NSIE reported in 1995, risks to information systems are multiplying "because of the increasing sophistication of the intruders and the more advanced methods of attack [and] the tools available to intruders are increasingly automated, easy to use, and effective."[15] The OMNCS has observed that "[m]any of these sophisticated tools are widely available to any intruder at any skill level [and] ... are available to all electronic intruders via the Internet and computer bulletin board systems."[16]

Making matters worse, there is increasing evidence that even those intruders with limited computer skills are accessing tools via the Internet and launching attacks against information systems. In its report to the U.S. Senate Permanent Subcommittee on Investigations, for instance, the GAO reported that "informal hacker groups, such as the 2600 club, the Legions of Doom, and Phrackers Inc., openly share information on the Internet about how to break into computer systems. This open sharing of information combined with the availability of user-friendly and powerful attack tools makes it relatively easy for anyone to learn how to attack systems or to refine their attack techniques."[17] In this manner, intruders have wide access to attack tools and techniques via the Internet and use the connectivity provided by the U.S. information infrastructure and, increasingly, a global information infrastructure as a potential avenue of attack. Those attacks are not limited by geographic boundaries.

Paradoxically, organizations tend to respond at the local level, protecting specific systems or networks while not being fully cognizant of network-wide or infrastructure-wide issues. When solutions are developed, they are often tailored to unique system or network configurations and do not address the larger concern of intruders using similar techniques to exploit systems owned and operated by different companies. Network-wide or infrastructure-wide protections are generally not used in any of the critical infrastructures, and there is no incentive (and a significant amount of risk) for companies to share sensitive intrusion information with other companies or the Government until major incidents occur (and not always even then). In addition, a majority of dollars being spent on network security by Government and industry focus on reactive technology and systems (i.e., detection and response). Comparatively little spending could be identified that was specifically targeted at proactive technologies in the areas of prevention and mitigation. Therefore, the subgroup found that:

---

15 An Assessment of the Risk to the Security of the Public Network, The Joint NSTAC-Government Network Security Information Exchange, February 1995, Section 3□Threat.

16 The Electronic Intrusion Threat to NS/EP Telecommunications: An Awareness Document, Office of the Manager, National Communications System, September 1994.

17 Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, General Accounting Office, May 15, 1996, p. 14-15.

- There is an inconsistent understanding and recognition of the electronic intrusion threat in the public and private sectors. A common theme in the subgroup's deliberations was the need to raise the national consciousness to the risks associated with electronic intrusions. Vendors indicated that some organizations take intrusions seriously and spend considerable sums to protect their networks while others take only minimal or suspect precautions.

5.2 Technology

Intrusion detection systems are being required to operate in rapidly changing network environments. Organizations are migrating from centralized, legacy systems characterized by mainframes to more open, networked, and distributed systems. Internal systems are being linked via intranets and enterprise networks to improve employee productivity and communications. Organizations are also using the Internet to improve their competitive advantage in the marketplace, complete electronic transfers, market products to wider customer bases, and exchange information in real-time. System users also are gaining access to a wider range of applications from their desktop. Although these activities are advantageous in terms of empowering employees by giving them access to a wider array of applications, such processes can make it more difficult for network and security managers to control access and use of those systems. Although these benefits are business imperatives, the subgroup identified several intrusion detection technology R&D issues that need to be considered from an NS/EP perspective.

5.2.1 Network Control Elements

Through analysis of survey responses and discussions with end users, the subgroup determined that intrusion detection technology R&D seldom focused on the telecommunications infrastructure and its key controlling elements (or for that matter on other critical infrastructures and their control elements). Many of the IDSs being used were developed and tailored to meet the needs of host systems operating in unique environments (e.g., UNIX, Novell, Microsoft NT). Although current IDSs detect some intrusions into specific systems, there has not been a great deal of focus on the network control systems that support the operation of the telecommunications infrastructure. There are critical components—Signaling System 7 (SS7), Signal Transfer Points (STPs), and Synchronous Optical Network (SONET)—that if attacked or exploited could result in a situation that threatened the security and reliability of the telecommunications infrastructure. Furthermore, there are network control elements (e.g., OAM&P in telecommunications, supervisory control and data acquisition systems (SCADA) for some other infrastructures) that may be targeted by potential intruders interested in launching denial of service attacks.

Given concerns about critical infrastructure protection, there is clearly a need to focus intrusion detection R&D on the network control and switching elements of the telecommunications and other critical infrastructures. Specifically, the subgroup found:

- Much of the intrusion detection technology R&D to date has focused on intrusions into host-based computer systems rather than investigating technologies and techniques to detect intrusions into sensitive network control elements. As critical infrastructures and their network control elements like OAM&P and SCADAs are interconnected with other systems and, therefore, become more attractive targets, there is a need to broaden current and planned R&D activities focused on standard network control systems.

5.2.2 Scaleable Systems

As described previously, many of the current intrusion detection systems deployed today were developed to operate in a host-based environment, capturing intrusions into a limited number of network nodes. As network interconnections increase, those systems generally are not able to expand their functionality to examine thousands of network nodes. The increasing complexity of systems and the business imperative to rapidly interconnect with other networks and the Internet have created a situation where intruders may be able to exploit vulnerabilities in one system to gain access to other, more sensitive systems. The subgroup determined that if IDSs were to meet the changing needs of the end user communities, they must be sufficiently scaleable to provide functionality across networks as the number of nodes increased. Specifically, the subgroup found:

- Many of the deployed IDSs are unable to scale to the large environments characterized by thousands of network nodes, which limits their ability to detect intrusions effectively across different platforms, applications, networks, and infrastructures.

5.2.3 Standards, Testing, and Validation

One topic that continually emerged in analyzing survey responses and in discussing intrusion detection technologies with the private sector was the need for standards, testing, and validation procedures to allow organizations to verify the capabilities of their IDSs. For example, several vendors and end users noted that there was no standardized format to collect and analyze audit reports. That inconsistency might make it more difficult for organizations to:

- Develop measures of performance in comparing products
- Integrate new IDSs with existing (and successful) products already being used
- Recognize intrusions when using new systems and products
- Require the retraining of employees to perform the same functions when new systems or products are purchased.

Vendors and end users also reported that a key factor in using IDSs is to establish a high level of confidence in their ability to perform reliably in detecting intrusions. Standards and testing can provide users with a means by which to determine how effective IDSs are in meeting their specific requirements. In considering the topics of standards, testing, and validation, the subgroup found:

- There is a need for large-scale testbeds to enable Government and private sector organizations to test IDSs in a more realistic environment. The development of dedicated networks to test IDSs and other products would be an expensive undertaking, requiring the creation of a diverse and complex network that would perform functions similar to those performed by telecommunications carriers.

- There is a need to develop standardized audit, alert, and reporting formats that allow organizations to more effectively compare intrusion information and develop metrics.

- There is general agreement on the need to develop test-case scenarios to assist organizations in testing their intrusion detection systems against a standard set of attack methodologies and other anomalies.

- There is a need for product evaluation criteria that provides end users with standard measures of performance and allows for product comparisons.

- There is a desire in both the research community and among end users to establish an independent laboratory to perform a thorough, careful, and realistic evaluation of intrusion detection systems and products.

- To adequately test and certify intrusion detection systems, a laboratory would need to develop a repository of attack scripts, profiles, and patterns to generate the standard test-case scenarios.

5.2.4 Metrics

Metrics are a topic closely related to standards, testing, and verification. Many organizations with IDSs do not analyze, compile, and record intrusion information on a continuing basis. These incidents often are handled case-by-case, and the related information is not retained unless law enforcement must become involved. Failure to compile intrusion information makes it extremely difficult to develop metrics. The development and use of standard metrics would enable organizations to baseline the number of intrusions they were experiencing and calculate the overall risk to their business. The subgroup found that industry and Government working together to develop metrics would assist end users to:

- Determine the levels of threat against their system

- Make a strong business case for investing in IDS and other security products

- Test IDS to measure performance

- Provide data to develop scenarios

- Compare vendors and products to determine those best suited to meet their requirements.

However, the subgroup also noted that open access to metrics of this type could provide an equally effective tool for hackers and electronic intruders. Electronic intruders could use those metrics as tools by which to measure their effectiveness in evading IDSs.

5.2.5 False Alarms

The subgroup identified the preponderance of false alarms as a major performance problem in current intrusion detection systems. To ensure that IDSs are used more effectively, system administrators and security practitioners must have confidence in their performance. These systems must perform with a high degree of certainty if organizations are to depend on their accuracy on a daily basis. Furthermore, the systems must be relatively low maintenance. If IDSs return false positives regularly, confidence in the system's ability may erode. The ultimate result might be a business decision to stop using the system because it is too time consuming to respond to false intrusion alerts. On the other hand, false negatives (failures to detect an intrusion) can also cause an organization to underestimate the level of threat to its systems and networks. Specifically, the subgroup found that:

- Reports indicate that false alarms are the primary reason organizations do not use intrusion detection systems or disable important but expensive elements of those systems.

- The development of common standards, testing and verification procedures, and metrics can provide ways to eliminate both false positives and false negatives.

5.2.6 New Attack Profiles

Many IDSs used today were designed to detect only those attacks that are outside of the normal pattern of behavior or violate a rule established by the system. Those techniques often rely on post-attack analysis of patterns or signatures that, after they are incorporated into the IDSs, will allow it to recognize that an attack has occurred or is occurring. As intruders uncover new vulnerabilities and use increasingly sophisticated attack tools, these systems may not be flexible or intelligent enough to distinguish between normal network behavior and anomalous behavior. Specifically, the subgroup found that:

- Potential intruders are sharing vulnerability information faster than the end users can patch holes. Many successful attack scripts are being automated to allow less skilled individuals to attack known vulnerabilities. The subgroup identified a need to develop IDSs that can recognize and respond to these new attack profiles.

- There is a need for a cooperative approach between Government, industry, and academia to share new attack methodologies, tools, and techniques to ensure that intrusion detection systems are prepared for all types of electronic intrusions.

5.2.7 Real-Time Alerts

Most IDSs available today analyze audit and alert records and develop profiles and patterns of behavior after the fact. Those profiles and patterns of behavior are subsequently incorporated into rule-based systems to recognize future attacks. Even in those instances where alerts are issued in near real-time, however, valuable time can be lost and an intruder's trail can go cold. Contributors to the report generally agreed that the development of a real-time intrusion detection capability would be necessary to immediately identify intrusions and issue real-time alerts that might prevent or limit network damage or exploitation. Specifically, the subgroup found that:

- There is a significant requirement for IDSs that can issue immediate alerts as the intrusions occur. This would ensure a minimal effect (damage or exploitation) on the network and allow for immediate response to intrusions, thereby limiting financial loss.

5.2.8 Damage Assessment and Response

Although IDSs are readily available for alerting organizations that they are being attacked, no systems appeared to provide them with an automated damage assessment and response capability. Advanced damage assessment and response tools could provide organizations with an ability to determine the extent of an intrusion and its potential impact on the network. Specifically, the subgroup found that:

- End users desire IDSs and other network security products that can assess the level of damage to the system.

- The lack of damage assessment and response features on intrusion detection systems limits the flexibility of end users to implement responses that correspond to the appropriate level of threat.

5.3 The Human Element

Researchers, vendors, and end users reported a general lack of public understanding about what constitutes an intrusion and the risks associated with intrusions. In any organization, the detection and reporting of an intrusion depends on each employee. Instances were cited where an employee failed to recognize when an intrusion was occurring or had occurred. Others may not even be aware of what an intrusion looks like. Even if it is determined an intrusion has occurred, organizational processes and procedures for alerting the appropriate officials of the incident might be confusing or poorly defined. Furthermore, several contributors to the study reported that the possibility existed that individuals might cover up an intrusion to avoid disciplinary actions from their employer.

5.3.1 Education, Training, and Awareness

Although technology will improve efforts to detect intruders, humans remain an essential element of the overall network security process. If administrators, operators, and users are not sufficiently trained and educated to recognize the need for intrusion detection and to operate IDSs and fail to recognize intrusions, the efficacy of technological advances may be severely limited. Given the range of possible problems inherent to human involvement, one of the best defenses against intrusions is to thoroughly train and educate the workforce to prevent, detect, and respond to intrusions. In addition, the subgroup found that:

- Effective intrusion detection efforts will require significant Federal and private sector investments in education, training, and awareness. Although network security technologies provide end users with tools to detect and respond to intrusions, there is also a need to make all system users aware of electronic intrusion risks and ensure they are adequately educated and trained to fully implement their organization's network security policies and procedures.

- There is clearly a need for IDSs that are sophisticated, automated, intuitive, and easy to use and understand.

- It was considered imperative that end users have access to products and tools comparable with those being deployed against them by hackers and other intruders.

5.3.2 Law Enforcement Requirements

Another topic that emerged during the subgroup's deliberations was the need for IDSs to be compatible with law enforcement requirements. Specifically, the subgroup found that:

- Current intrusion detection systems are not designed to collect and protect the integrity of the type of information required to conduct law enforcement investigations.

- There is a lack of guidance to employees as to how to respond to intrusions and capture the information required to conduct a law enforcement investigation. The subgroup discussed the need to develop guidelines and training materials for end users that will make them aware of what information law enforcement requires and what procedures they use to collect evidence on an intrusion.

5.4 Summary of Findings

In its study and deliberations, the IDSG identified three sets of issues related to intrusion detection technology R&D, specifically:

- **National Policy**
  The subgroup determined that the processes by which intrusion detection technologies were researched, developed, and moved from the laboratory to the marketplace in the most expeditious manner were unclear. The members agreed on the need for a

national technology policy that would articulate a Federal vision for intrusion detection (and other network security) technologies and would establish Federal research objectives, targets, and priorities. Furthermore, that policy should ensure that all R&D projects would be coordinated among Federal departments and agencies and that a cooperative relationship between Government, industry, and academia is supported.[18]

- **Technology**
  The overarching concern with respect to intrusion detection technologies is that R&D has focused on detecting intrusions in the host or multihost environment rather than the network-wide and infrastructure-wide levels. Much of the technology being researched today will not address the increasing concerns of intrusions into the sensitive network control and switching elements that support many of the critical infrastructures. As the private sector continues to automate even its most sensitive control elements, the subgroup recognized the importance of establishing testbeds and laboratories to develop standards, metrics, testing & verification procedures, and product certification that will raise the level of confidence in the private and public sectors to the effectiveness of intrusion detection technologies.

- **The Human Element**
  There is a general lack of awareness of the risks associated with electronic intrusions and funding to educate and train end users to recognize and respond to intrusions. Furthermore, there are no established procedures for collection of data and other evidence to support investigation and prosecution of intruders.

6.0 RECOMMENDATIONS

Protecting critical infrastructures is a growing national priority, and the U.S. information infrastructure provides services essential to the operation and control of all infrastructures. Ensuring the continued operation of the U.S. information infrastructure and its key components is a national security requirement and business necessity. Infrastructure failures could hamper military operations, disrupt the national economy, and erode the public's confidence. Therefore, it is in the interest of all parties to bolster the capability to detect electronic intrusions. To adequately meet this requirement, further R&D in intrusion detection technologies is essential. This section outlines the recommendations developed by the IDSG in response to gaps in intrusion detection technology R&D. The subgroup believes these recommendations will bolster the research and development of intrusion detection technologies and ensure that evolving NS/EP requirements are satisfied.

6.1 Promulgate a National Technology Policy to Address Intrusion Detection

In its analysis of intrusion detection technology R&D, the IDSG identified several deficiencies. First was the lack of a national policy to direct the research and development of

[18] In its deliberations on national policy, the subgroup considered the concurrent efforts of the PCCIP to examine potential policy, technical, and R&D issues related to emerging cyber threats.

intrusion detection technologies that offered promise in combating electronic intrusions and in protecting critical national infrastructures from attack. The subgroup also recognized the broader requirement for a national technology policy to foster the development of more robust and advanced network security technologies.

Therefore, the subgroup recommends the President consider establishing a national technology policy addressing intrusion detection to:

- **Establish a Federal vision to encourage the development of intrusion detection technologies**
  The subgroup determined that intrusion detection technology R&D appeared to be fragmented and uncoordinated. A national policy could outline a Federal vision for encouraging the development of intrusion detection technologies to include research objectives, priorities, and targets.

- **Increase programmatic funding of intrusion detection technology R&D**
  The subgroup observed that intrusion detection technologies appeared to be a low priority in terms of funding in relationship to other Federal efforts to develop IAW/command & control centers. A national policy could better establish Federal budgetary priorities to ensure a balanced approach to combat electronic intrusions that includes prevention, detection, response, and mitigation measures.

- **Foster partnerships with industry and academia**
  Because the majority of the Nation's critical infrastructures are owned and operated by the private sector, it is important that any national policy recognize the importance of competitive forces in shaping the R&D of intrusion detection technologies. To this end, a national policy for intrusion detection could: foster the establishment of partnerships between Government, industry, and academia; maximize Federal investments to ensure the greatest return; provide incentives to the private sector; and encourage competition to increase pace of development.

- **Raise the national consciousness**
  There is an uneven understanding of the risks associated with electronic intrusions. Cyber attacks, regardless of the motivation or intent, have the potential to cause great national security or economic harm. A national policy could provide the framework by which to make the public more aware of the risks associated with electronic intrusions.

6.2 Establish an Interagency Working Group for Intrusion Detection

In addition to promulgating a national technology policy, there remains a need for better coordination of existing and planned Federal intrusion detection technology R&D projects. The Federal Government has placed a great deal of emphasis on investing in intrusion detection initiatives, but many of those efforts appear to be disparate and fragmented. For that reason, the

IDSG recommends the President consider establishing an interagency working group composed of those organizations already actively involved in intrusion detection technology R&D to:

- **Establish Federal R&D targets and priorities**
  An interagency working group could maximize returns on the Government's investments by establishing common research objectives, targets, and priorities.

- **Coordinate Federal program management and oversight**
  An interagency working group could provide a formal mechanism for information exchange in the Federal Government on research projects, available funding mechanisms, and eliminate duplication of effort.

- **Balance Federal funding between basic research and applied development**
  An interagency working group could be tasked to strike a better balance between basic research initiatives and efforts to apply and prototype existing technologies into innovative solutions to detect electronic intrusions.

- **Identify and champion promising intrusion detection technologies**
  An interagency working group could be the focal point for developing criteria and selecting projects and emerging technologies that have the potential to be commercially viable and establishing technology transfer programs to rapidly prototype or test those technologies in a realistic, commercial environment.

6.3 Increase R&D Funding for Control Systems of Critical Infrastructures

The U.S. information infrastructure and other critical national infrastructures rely on automated network control systems to manage the essential operations of their respective infrastructures. In the telecommunications industry, for example, several key systems (i.e., OAM&P, SS7) support the control or switching of the public switched network. As owners and operators of critical infrastructures increasing seek to exploit the benefits of information technology (i.e., linking to the Internet, intranets, corporate LANs), their sensitive control and switching elements may or may not be exposed to increase risk. Regardless, those systems represent the "crown jewels" of critical infrastructures and as such will be attractive targets for those interested in attacking or exploiting an infrastructure.

To date, there has been little research and development of intrusion detection technologies designed to detect intrusions into those systems. More often than not, IDSs are designed to detect intrusions into host-based systems. The subgroup also identified a few projects focused on researching detection tools for network-wide or infrastructure-wide problems. However, this research is in its formative stages and requires significant attention. Given the President's interest in infrastructure protection issues, the IDSG recommends the President consider directing the appropriate Federal departments and agencies to:

- **Increase funding for Federal R&D initiatives focused on control systems for critical infrastructures**

The subgroup recognized the importance of funding Federal R&D initiatives focused on developing technologies, systems, and tools specifically designed to detect intrusions into network control and switching systems, which are vital to maintaining the continued operation of critical infrastructures.

6.4 Encourage Cooperative Development Programs

A majority of the Nation's critical infrastructures are owned and operated by the private sector, and their security measures are increasingly driven by market imperatives not national security requirements. As such, there is a need for Government to work closely with industry and academia to develop cooperative programs and solutions to electronic intrusions. The IDSG recommends that the President consider tasking the appropriate Federal departments and agencies to encourage cooperative development programs including Government, industry, and academia. The focus of those development programs could be to:

- **Maximize use of limited resources**
  Given fiscal and budgetary constraints in Government, industry, and academia, all stakeholders need to work together to identify public and private resources invested in intrusion detection technology R&D and apply resources where they will have the most impact.

- **Establish standards, testing and verification procedures, and metrics**
  All parties must work closely through existing standards bodies and other fora to establish common standards, testing and verification procedures, and metrics. The lack of standards, testing, verification, and metrics makes it difficult for organizations to develop accurate intrusion thresholds, measure system performance, integrate new systems with older IDSs, and compare products. One possible solution is to develop independent laboratories to test and certify products and to develop standard test-case scenarios to verify the capabilities of IDSs.

- **Identify protection schemes**
  Government and industry may use or experiment with different protection schemes, technologies, and risk management approaches to limit the potential effects of electronic intrusions. There need to be cooperative programs that allow those organizations to exchange information on those schemes and techniques to develop "best practices" in protecting networks from intrusions.

- **Fund large-scale testbeds**
  During the course of this study, many parties noted the importance of developing large-scale testbeds to accurately test intrusion detection technologies in a realistic environment. Developing such testbeds will be an expensive undertaking, requiring the combined resources and expertise of Government, industry, and academia.

- **Identify incentives to foster competition in intrusion detection**

The Government needs to work closely with industry to identify R&D incentives to foster competition in the intrusion detection marketplace that will speed the pace of development and lead to innovative solutions.

- **Identify methods to assist law enforcement**
  Many of the IDSs in the field today are not conducive to collecting the requisite evidence to conduct a law enforcement investigation. Government and industry must work together to develop and promote technologies that allow for real-time alerts and damage assessment while collecting information essential to investigate and prosecute those responsible for illegal intrusions.

6.5 Continue to Examine Feasibility of an R&D Consortium

The IDSG also recommends the Network Group continue to work closely with the U.S. Government to examine the feasibility of establishing a joint industry-Government R&D Consortium focused on network security technology issues, as stated in its 1998 work plan.

ANNEX A

IDSG Survey Letters

Sample: To Universities and Research Organizations

Joe Smith
State University
Computer Sciences Program
University Park, OH 12345

To Mr. Smith:

The purpose of this letter is to request information regarding detecting intrusions into computer and information systems for the President's National Security Telecommunications Advisory Committee (NSTAC). NSTAC is composed of 30 senior executives of major United States corporations from the telecommunications and information systems industries, and major corporations which are users of those technologies. In general, they advise the President of the United States on policies, technical matters and the implications of emerging technologies where they impact or relate to National Security and Emergency Preparedness (NS/EP). Enclosed is the most recent copy of the NSTAC fact sheet which will provide more background on the organization.

Recently, at the request of the President, much of their work has been focused on issues related to protecting the information and telecommunications systems on which our critical infrastructures are growing ever more reliant. As part of that focus, NSTAC formed an Intrusion Detection Subgroup (IDSG) and charged that group with examining current and future Government, industry, and academic research and development activities to: (1) determine the shortcomings in the Nation's capabilities to be aware of intrusions, (2) understand the focus of major intrusion detection research projects that are planned or underway, and (3) evaluate the significance and make recommendations to the President both on work that is being done and that which is not being done. The scope of this effort is not limited to information technology affecting only telecommunications systems.

Through this letter, we are requesting your assistance in this matter. We would like your responses to the following questions:

1) What are your views of the current global challenges and shortcomings in the area of intrusion detection?

2) Are you actively pursuing a research program in the area of intrusion detection?

3) If so, what is the focus or proposed methodologies for your intrusion detection research efforts?

4) How large (time, people, dollars, etc.) is your project and is it fully funded?

5) What other research entities are you collaborating with on this project, if any?

6) How long have you been working in the intrusion detection area, and has funding been generally increasing or decreasing?

7) Can you recommend anyone else that we should contact with this questionnaire?

8) The IDSG is primarily interested in assessing what types of research are being done, and what areas could used additional work. Please give us your thoughts on this issue.

9) Finally, could you provide a short (1 page) abstract which describes your research project?

Mr. Stephen Mencik from the Office of the Manager for the National Communications System (OMNCS) will be coordinating the data collection for this survey. If requested, personal and group affiliation with the answers can and will be kept confidential. Proprietary data should be marked as such. Please forward your responses to Mr. Mencik, by April 8, 1997, if possible. His mailing address is:

National Communications System
ATTN: N5 / Stephen Mencik
701 S. Court House Road
Arlington, VA 22204-2198

Responses may also be sent via E-mail (preferred method) to menciks@ncs.gov, or via fax to (703) 607-4826. If you have any questions regarding this matter, please call Mr. Mencik at (703) 607-6115.

We sincerely appreciate your assistance in this important National endeavor.

James Bean, GTE
NSTAC IDSG chair

Encl: NSTAC Fact Sheet

Electronic Mail to NSTAC Representatives Requesting Assistance

The NSTAC's Network Security Group has recently formed an Intrusion Detection Subgroup (IDSG) to "determine and recommend necessary NSTAC action with regard to Intrusion Detection, including technological, operational and joint industry/government issues." The focus is on intrusions into the Nation's telecommunications infrastructure as well as the potential impact such intrusions could have on other critical infrastructures.

The subgroup is looking at the definitions, research, and policies on intrusion detection. The initial step in our work plan is to solicit help from the Industry Executive Subcommittee members with regard to intrusion detection issues in their companies. To that end, the IDSG would like you to address the following questions:

1. How do you define "intrusion," "intrusion detection," and "indications, warning, and assessment (IWA)" in your network or company?

2. As you have monitored your networks to detect intrusion attempts, what tools and techniques have you seen intruders use to try to gain unauthorized access to your networks?

Please address questions 3-5 from a communications network control system standpoint (i.e., the focus is on the operations, administration, maintenance, and provisioning systems used to control your networks):

3. What intrusion detection capabilities does your company currently employ?

4. What intrusion detection R&D is your company currently pursuing?

5. What additional R&D should be pursued in the area of intrusion detection?

The IDSG would appreciate specificity in answering the above questions commensurate with the necessary confidentiality you must maintain.

It would be preferable to have any responses before our next meeting on December 4. If that is not possible, please try to have them to us by Friday, December 13.

We appreciate your help in this matter.

ANNEX B

Intrusion Detection Subgroup Members and Government Contributors

Intrusion Detection Subgroup Members

GTE	James Bean (Chair)
AT&T	Larry Nelson
CSC	Guy Copeland
EDS	James Hawkins
GTE	David Gorman
ITT	David Kelly
ITT	Stuart Cohen
NORTEL	John Edwards
SAIC	Matthew Devost
SAIC	Paul Proctor
TRW	Ann Marmor-Squires

Government Contributors

DARPA	Teresa Lunt
DISA	Benjamin Gaddy
DOE	Carl Piechowski
NCS	Stephen Mencik
NSA	Richard Brackney
NSA	Blaine Burnham
Sandia National Laboratories	Fred Cohen
Treasury	David Dingman

Staff Support

BoozAAllen & Hamilton	Dave Sulek
BoozAAllen & Hamilton	James Truitt
BoozAAllen & Hamilton	Jaton West

ANNEX C

Organizations Contributing to IDSG Efforts

Presentations

- Fred Herr, OMNCS (12/4/96)
- Ben Gaddy, DISA (12/4/96)
- Dave Gorman, GTE (12/4/96)
- Lt Col Perry Luzwick, JS-J6 (12/19/96)
- Dick Brackney, NSA (12/19/96)
- Ed Keefe, TREAS (12/19/96)
- David Kelly, ITT (1/8/97)
- Tom Longstaff, CERT-CC (3/3/97)
- George Spix, Microsoft (4/17/97)
- Paul Proctor, SAIC (4/17/97)
- Ron Knode, CSC (4/17/97)
- Bob Huffman, The WheelGroup (5/15/97)
- Bob Kane, Intrusion Detection, Inc. (5/15/97)
- Fred Cohen, Sandia National Laboratories (5/15/97)

Survey Responses

- ATM Research Consortium
- Bellcore
- Boeing Defense and Space Group
- Carnegie Mellon University
- Columbia University
- GTE Government Systems
- Lincoln Laboratory, DOE
- MCNC
- MIT Artificial Intelligence Center (2)
- The MITRE Corporation (2)
- Odyssey Research Associates
- The Open Group Research Institute
- Seven Locks Software, Inc.
- SRI Artificial Intelligence Center
- SRI Computer Science Laboratory
- Touch Technologies, Inc.
- Trusted Information Systems, Inc (2)
- University of California-Davis
- University of Illinois at Urbana-Champaign
- University of Maryland
- University of Southern California

ANNEX D

Glossary

Assessment
The analysis of indications to determine the likelihood, nature, and potential of a threat.

Autonomous
Self-contained and independent agents in a system.

Detection
Comparing normal patterns of behavior and identifying abnormalities that could be intrusions.

End Users
For the purposes of the IDSG study, end users were defined as those individuals responsible for operating, managing, and administering networked systems.

Expert Systems
Expert systems are driven from an encoded rule base. The expert system does not try to differentiate normal from anomalous activity. Rather, it applies the rules individually or in combination to ensure that all users are within their privileged rights.

False Negatives
Failure to identify an intrusion that has actually occurred.

False Positives
Identifying an event as an intrusion when in fact one has not occurred.

Heterogeneous Environment
An environment wherein networks can be linked to other networks across a variety of platforms.

Infrastructure
The basic facilities, equipment, and operating instructions needed for a system to operate.

Intrusion
Unauthorized access to, and/or activity in, an information system.

Intrusion Detection
The process of identifying that an intrusion has been attempted, is occurring, or has occurred.

Indications
Information that suggests a threat. Indications include explicit evidence that an intrusion has occurred and implicit evidence revealing the interests, intentions, and capabilities of the threat.

Information Assurance
Protection of key public and private elements of the NII from exploitation, degradation, and denial of service.

Information Operations
Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information System
The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

Information Warfare
Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

Mitigation
Actions taken to make the effects of intrusions less severe or harmful.

Monitors
Passive systems that continually analyze the data presented to them. Similar to antivirus functions in that they can detect what has been defined to them.

Prevention
Measures to preclude, deter, or handicap the likelihood of a successful intrusion.

Profiling
Analysis of the flow of data in the system to determine "normal" and "abnormal" patterns of behavior.

Reporting
The act of notifying the appropriate personnel of a suspected intrusion. Reporting can be periodic printed reports of event information based on a timing mechanism or asynchronous alerts based on a defined event trigger.

Responses
An action or series of actions constituting a reply or reaction against an attempted or successful intrusion.

Rule-Based Access
An access approach that establishes a highly protected system under the control of the system administrator. This approach identifies unauthorized attempts to change permission levels or exceed system permissions.

Scanners
Proactive and predictive in nature, seeking out security holes and signs of intrusion. Scanner capabilities include checking integrity and policy compliance and detecting known vulnerabilities, unauthorized hardware and software, and code changes.

Threats
A potential undesirable event, malicious or not, of (1) compromise (i.e., theft of valuable or sensitive information or services), (2) corruption of information and information services, or (3) denial of service by degradation and blocking of data, processing, or communications or an entity possessing the capability and intent to cause the above.

Vulnerabilities
Weaknesses within an operating system that might allow an intrusion to occur.

Warnings
An advisory of the results of the assessment, likely target(s), and recommended actions.

ANNEX E

Acronyms

Acronyms

DARPA	Defense Advanced Research Projects Agency
DISA	Defense Information Systems Agency
DoD	Department of Defense
GAO	General Accounting Office
IAW	Indications, Assessment, and Warning
IA	Information Assurance
IW	Information Warfare
IPTF	Infrastructure Protection Task Force
IDS	Intrusion Detection Systems
IDSG	Intrusion Detection Subgroup
NCS	National Communications System
NCC	National Coordinating Center for Telecommunications
NII	National Information Infrastructure
NIST	National Institute for Standards and Technology
NSA	National Security Agency
NS/EP	National Security and Emergency Preparedness
NSIE	Network Security Information Exchange
NSTAC	President's National Security Telecommunications Advisory Committee
OAM&P	Operations, Administrative, Maintenance, and Provisioning
OMNCS	Office of the Manager, National Communications System
PCCIP	President's Commission on Critical Infrastructure Protection
PSN	Public Switched Network
R&D	Research and Development
SCADA	Supervisory Control and Data Acquisition
SS7	Signaling System 7
STP	Signal Transfer Point
SONET	Synchronous Optical Network