**SANDIA REPORT**
SAND2010-4766
Unlimited Release
Printed September 2010

# National Cyber Defense High Performance Computing and Analysis: Concepts, Planning and Roadmap

Curtis M. Keliiaa and Jason R. Hamlet

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

**NOTICE:** This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2010-4766
Unlimited Release
Printed September 2010

# National Cyber Defense High Performance Computing and Analysis: Concepts, Planning and Roadmap

Curtis M. Keliiaa
Advanced Networking Integration

Jason R. Hamlet
Assurance Technology and Assessments

Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS0806

**Abstract**

There is a national cyber dilemma that threatens the very fabric of government, commercial and private use operations worldwide. Much is written about "what" the problem is, and though the basis for this paper is an assessment of the problem space, we target the "how" solution space of the wide-area national information infrastructure through the advancement of science, technology, evaluation and analysis with actionable results intended to produce a more secure national information infrastructure and a comprehensive national cyber defense capability.

This cybersecurity High Performance Computing (HPC) analysis concepts, planning and roadmap activity was conducted as an assessment of cybersecurity analysis as a fertile area of research and investment for high value cybersecurity wide-area solutions. This report and a related SAND2010-4765 *Assessment of Current Cybersecurity Practices in the Public Domain: Cyber Indications and Warnings Domain* report are intended to provoke discussion throughout a broad audience about developing a cohesive HPC centric solution to wide-area cybersecurity problems.

# ACKNOWLEDGMENTS

Appreciation is due to the following individuals for their contributions in the development of this report.

Tan Chang Hu, 05627 Assurance Tech & Assessments
David G. Robinson, 01415 Computer Science & Informatics
Anand Ganti, 09336 Advanced Networking Integration
Vitus J. Leung, 01415 Computer Science & Informatics
Keith Vanderveen, 08961, Manager, Scalable Computing R&D
Robert A. Ballance, 09328 Scientific Computing Systems
Steve A. Gossage, 09336, Advanced Networking Integration
Kevin Pedretti, 01423, Computer Systems Analysis

# CONTENTS

1. Executive Summary ..... 7

2. Introduction ..... 9
   2.1 Introduction ..... 9
   2.2 Organization ..... 10

3. Priority Problems, Actionable Results, and Paths to Realization ..... 11
   3.1 Defining the Cyberterrain Problem Space ..... 11
      3.1.1 Cyberterrain Problem Space: Assessment Conclusions ..... 17
   3.2 Areas of Impact, Priority Problems, Research, and Actionable Results ..... 17
   3.3 Fundamental Relationships, Integration and Potential Benefits ..... 22
      3.3.1 Fundamental Relationships, Integration and Potential Benefits: Assessment Conclusions ..... 34

4. Wide-Area Cybersecurity Design Space ..... 35
   4.1 Cybersecurity in an Ecosystem ..... 35
      4.1.1 Cybersecurity in an Ecosystem: Assessment Conclusions ..... 37
   4.2 Wide-Area Conceptual Design Space ..... 38
      4.2.1 Wide-Area Conceptual Design Space: Assessment Conclusions ..... 45
   4.3 Related Impacts in the National Threat and Defense Posture ..... 46
      4.3.1 Related Impacts within the National Threat and Defense Posture: Assessment Conclusions ..... 51

5. Solution Space Concepts of Operations and Roadmaps ..... 53
   5.1 Solution Space Concepts of Operation ..... 53
      5.1.1 Value Based Information Protection Concept of Operations ..... 53
      5.1.2 Cyber Personification Schema Concept of Operations ..... 54
      5.1.3 Distributed Detection, Notification and Response Concept of Operations ..... 56
      5.1.4 Cyber Adaptive Response Architectures Concept of Operations ..... 58
      5.1.5 Scalable Cyber Threat Definition Concept of Operations ..... 60
      5.1.6 Federated Business Continuity Planning Concept of Operations ..... 61
      5.1.7 Solution Space Concepts of Operation: Assessment Conclusions ..... 66
   5.2 Roadmap with Quantifiable Goals and Objectives ..... 67

6. Challenges, Opportunities, and Conclusions ..... 73
   6.1 National Cyber Defense Challenges ..... 73
   6.2 Ten High Impact Opportunities ..... 74
   6.3 National Cyber Defense HPC Analysis Concepts, Planning and Roadmap: Conclusions 75

Distribution ..... 77

# FIGURES

Figure 1. Cyberterrain Assessment & Game Board Metaphor Development Process ..... 11
Figure 2. Cybersecurity Subject Matter Matrix ..... 12
Figure 3. Cyberterrain Game Board and Advanced Cyber HPC Analysis Area of Focus ..... 13

Figure 4: Cyberterrain Areas of Impact ..... 18
Figure 5: Cyberterrain Priority Wide-Area Problems ..... 19
Figure 6: Cyberterrain HPC Analysis Areas of Research ..... 19
Figure 7: Targeted Actionable Results of Cybersecurity HPC Analysis ..... 21
Figure 8: Areas of Impact, Priority Problems & Integrating Elements ..... 23
Figure 9: Areas of Impact, Priority Problems, Integrating Principles & Threads of Reasoning .. 24
Figure 10: Areas of Research, Actionable Results & Integrating Elements ..... 26
Figure 11: Areas of Research, Actionable Results, Integrating Principles & Threads of Reasoning ..... 27
Figure 12: Customer Objectives, Application, Function, Conceptual & Realization ..... 30
Figure 13: Conceptual Cyberterrain Wide-Area Threat Evaluation Environment ..... 40
Figure 14: Conceptual Cyberterrain High Speed Distributed Sensor Environment ..... 43
Figure 15: Conceptual Cyberterrain Distributed HPC Analysis Environment ..... 44
Figure 16: History Informs Our Future ..... 50
Figure 17: Conceptual Cyberterrain Cyber Adaptive Response Architecture ..... 59
Figure 18. Conceptual Scalable Cyber Threat Definition ..... 60
Figure 19: Federated BCP Command Structure ..... 62
Figure 20: Emergency Management and BCP Coordination ..... 64
Figure 21: Cyberterrain HPC Cybersecurity Analysis Roadmap ..... 67
Figure 22: Cyberterrain Possible Outcomes and Future Actionable Results ..... 68
Figure 23: HPC Complexity Analysis and Modeling & Simulation Desired Outcomes ..... 69
Figure 24: Localized Trusted Interface Connections Desired Outcomes ..... 70
Figure 25: Wide Area and Localized Trusted Interface Connections Desired Outcomes ..... 71
Figure 26: Identified Shared Risk and Mitigations Desired Outcomes ..... 72

## TABLES

Table 1. Cyberterrain Defense and Nomenclature Continuums ..... 14
Table 2. Threat Characteristics ..... 16
Table 3. Factors and Personification Risk Mitigation ..... 56
Table 4. Cyber Threat Levels and Severity Indicators ..... 58
Table 5. National Cyber Defense Quantifiable Objectives ..... 69

# 1. EXECUTIVE SUMMARY

This report exists in the larger context as the third in a series of three related reports. The first, *A Sensor Network Study* [1] provides a detailed description of sensor networks, which will likely be a critical component for collection, filtering, and initial analysis of cybersecurity data in distributed, high performance computing (HPC) oriented architectures. The second, *Assessment of Current Cybersecurity Practices in the Public Domain: Cyber Indications and Warnings Domain*[2] discusses current, unclassified cybersecurity practice and identifies abundant opportunity for HPC use. This report presents initial concepts, planning and a roadmap toward cybersecurity HPC analysis to alleviate the cybersecurity dilemma on a national scale.

We began conceptualization by organizing areas of concern in the cybersecurity domain:

1. Threat & Vulnerability
2. Safeguards and Countermeasures
3. Risk Management
4. Prevention and Protection
5. Information Management
6. Detection and Warnings
7. Investigation and Response
8. Leadership and Authority
9. Resource Requirements
10. Workforce and Defenders
11. Coordination and Communication
12. Science and Engineering
13. Evaluation and Analysis
14. Actionable Results

Note that HPC resides in the Science and Engineering, Evaluation and Analysis, and Actionable Results areas of concern. We then identified seven areas where HPC could positively impact the wide-area of the national information infrastructure cybersecurity domain:

1. Threat & Vulnerability
2. Safeguards and Countermeasures
3. Risk Management
4. Prevention and Protection
5. Information Management
6. Detection and Warnings
7. Investigation and Response

The cybersecurity domain is presented as a cyberterrain game board metaphor to portray a continuous lifecycle with human, organizational, legal, and technical interdependencies.

[1] SAND2009-6671 P A Sensor Network Study, January 2010
[2] SAND2010-4765 Keliiaa, C.M and Hamlet, J.R. *Assessment of Current Cybersecurity Practices in the Public Domain: Cyber Indications and Warnings Domain*, Aug. 2010

We identify seven priority wide-area problems in the wide-area cybersecurity domain:

1. Disjointed Response to Wide-Area and Multi Target Attack
2. Widely Dispersed and Fragmented Detection and Notification Capabilities
3. Ill-defined Government, Commercial, and Academic Roles and Responsibilities
4. Divided and Rigid Wide-Area Cyber Protection Posture
5. Unresolved Wide-Area Common and Shared Risks
6. Fragile Interdependent Wide-Area Critical Access and Operations
7. Unresolved Attribution of Attack and Compromise

We emphasize the solution space by presenting recommended areas of HPC research:

1. Trusted Connection and Automated Processes
2. Informatics, Statistics and Anomalous Behavior
3. Mathematics Analysis and Intrusion Detection
4. Complexity Science and Emergent Behavior
5. Modeling and Simulation
6. Analysis and Correlation Algorithms
7. Sociology and Psychology

and actionable results to resolve national information infrastructure scale problems:

1. Identification of Gaps and Vulnerabilities
2. Effective Response to Attack
3. Near Real-Time Notification of Infrastructure Attack and Information Compromise
4. Agile and Adaptive Defense
5. Identified Cross Domain Risks and Mitigations
6. Minimized Attack Surface
7. Assured Critical Access and Operations
8. Attribution of Attack and Compromise

Discrete subject matter areas of interest are examined and potential paths to realization are explored. We consider the cyberterrain in terms of complexity on the scale of an ecosystem and expand and define the wide-area cybersecurity design space in terms of threat evaluation, distributed sensor network, and distributed HPC analysis environments to show a conceptual, high-level cybersecurity architecture that is amenable to HPC. We draw attention to the century old USG legal framework governing privacy of communications within which cybersecurity practices must operate, and consider broadly applied concepts of operation for increased national cyber defense and information asset protection.

Coarse flowcharts illustrating relationships between research activities and desired outcomes accompany a preliminary long term roadmap based on recent technological gains in anomaly detection, advanced operating system virtualization, and Sandia's National Security Computing Center (NSCC). We conclude with a summation of national cyber defense challenges, opportunities and conclusions to help prioritize funding of future research.

# 2. INTRODUCTION

## 2.1 Introduction

There is a national cyber dilemma that threatens the very fabric of government, commercial and private use operations worldwide. Much is written about "what" the problem is and the cybersecurity industry has grown to international prominence in reaction to an ever increasing threat. Although the basis for this paper is an assessment of the problem space, we target the "how" solution space of the wide-area national information infrastructure through the advancement of science, technology, evaluation and analysis with actionable results intended to produce a more secure national information infrastructure and a comprehensive national cyber defense capability.

This cybersecurity High Performance Computing (HPC) analysis concepts, planning and roadmap activity was conducted as an assessment of cybersecurity analysis as a fertile area of research and investment for high value cybersecurity wide-area solutions. Areas of concern were considered as a game board metaphor to provide a fulsome "cyberterrain" description of the cyber problem domain. Cyberterrain areas of concern were identified as well as a subset of areas of impact that would benefit from particular areas of cybersecurity HPC research.

The areas of HPC research were first identified in a collaborative assessment [3] [SAND2009-7094 P] of the cybersecurity industry, HPC, and distributed sensor networks in the Cyber Indications and Warnings Domain (CIWD). These areas of research are considered computationally, large data-set, or time-to-solution intensive and of a nature appropriate to HPC analysis.

The reasoning, process and progressive development are shown with the intent to illuminate that the cyberterrain has evolved and increased in complexity on the scale of an ecosystem. The approach includes the assessment of several areas of importance:

1. Cyber Problem Space Domains of Concern
2. Areas of Impact, Priority Problems, Areas of Research, and Actionable Results
3. Fundamental Relationships, Integration and Potential Benefits
4. Cybersecurity in an Ecosystem
5. Wide-Area Conceptual Design Space
6. Related Impacts within the National Threat and Defense Posture
7. Solution Space Concepts of Operation
8. Roadmap with Quantifiable Goals and Objectives

Utilizing technological gains in anomaly detection, advanced operating system virtualization, and Sandia's National Security Computing Center (NSCC) the resultant roadmap defines a possible program path forward with quantifiable goals and objectives. Such roadmaps may be useful in prioritizing future research and funding efforts.

[3] SAND2009-7094 P Interim Report Task 1 Assessment of Current Cybersecurity Practices in the Public Domain: Cyber Indications and Warnings Domain, October 2009

## 2.2 Organization

The information herein is largely conceptual, although based on literature review of the cybersecurity industry, HPC systems and trends, and sensor network technologies. This document is accompanied by a report summarizing an assessment of current cybersecurity practices in the public domain. This accompanying report serves as the primary technical informational basis of this work, although additional review conducted for this national cyber defense concepts, planning and roadmap activity are noted within the text. Please refer to the *Assessment of Current Cybersecurity Practices in the Public Domain: Cyber Indications and Warnings Domain* [4]report for further technical discussion: Findings and Recommendations discuss the current state of the cyber security industry; HPC class of systems and benchmarks; trends; applications of cybersecurity to HPC; high speed sensor networks; algorithms; reference architectures and data models; Conclusions include a discussion of influencing factors in distributed cyber security computing systems; and recommended actions and potential areas of research to advance HPC cybersecurity applications.

The remainder of this document is organized as follows. In chapter 3 we define the cyberterrain problem space on the scale of the wide-area national information infrastructure in a game board metaphor, and present priority problems, actionable results, and paths to realization through HPC research. In particular, section 3.1 identifies 14 areas of concern in the cybersecurity domain; section 3.2 identifies a subset of these areas that might benefit from HPC analysis, identifies priority problems in each area, and recommends areas of HPC research and actionable results from that research that are closely aligned with the priority problems; and section 3.3 illustrates relationships between the areas of impact and the priority problems and actionable results.

Chapter 4 explores the conceptual wide-area design space. Section 4.1 introduces an ecosystem metaphor for cybersecurity analysis applicable to HPC oriented wide-area cybersecurity architectures and section 4.2 defines the wide-area cybersecurity design space in terms of a threat evaluation, distributed sensor network, and distributed HPC analysis environments to show a conceptual, high-level cybersecurity architecture that is amenable to HPC. Section 4.3 describes some current national cybersecurity policy and the historical legal context within which cybersecurity practices must operate and the difficulty in investigating and prosecuting cyber crime in an international environment.

Chapter 5 explores the solution space and expands the discussion beyond HPC analysis with several related wide-area concepts of operation. Section 5.1 presents concepts of operation related to value based information protection, cyber personification, distributed detection, notification and response, cyber adaptive response architectures, scalable cyber threat definition, federated business continuity planning. Section 5.2 presents a preliminary long term cybersecurity roadmap for progressive development of a wide-area cybersecurity HPC capability and coarse flowchart style roadmaps illustrating relationships between research activities and desired outcomes. Finally, chapter 6 presents a summation of preliminary national cyber defense challenges, opportunities, and conclusions to assist in prioritization of future work.

---

[4] SAND2010-4765 Keliiaa, C.M and Hamlet, J.R. *Assessment of Current Cybersecurity Practices in the Public Domain: Cyber Indications and Warnings Domain*, Aug. 2010

# 3. PRIORITY PROBLEMS, ACTIONABLE RESULTS, AND PATHS TO REALIZATION

## 3.1 Defining the Cyberterrain Problem Space

*Goal: Develop a game board metaphor illustrating "cyberterrain" areas of concern as applicable to the wide-area of the national information infrastructure.*

Figure 1 illustrates the cyberterrain assessment and development process followed to define the cyberterrain problem space on the scale of the wide-area national information infrastructure expressed in a game board metaphor. We began with a matrix of activity related to cybersecurity practices to assess requirements and scope of the "cyberterrain". The initial assessment considered the detection and warnings domain and investigation and response domain as predominate areas for improvement in the cyberterrain. An additional advantage of the game board metaphor is to give reference to the oft used "game changing" paradigm.

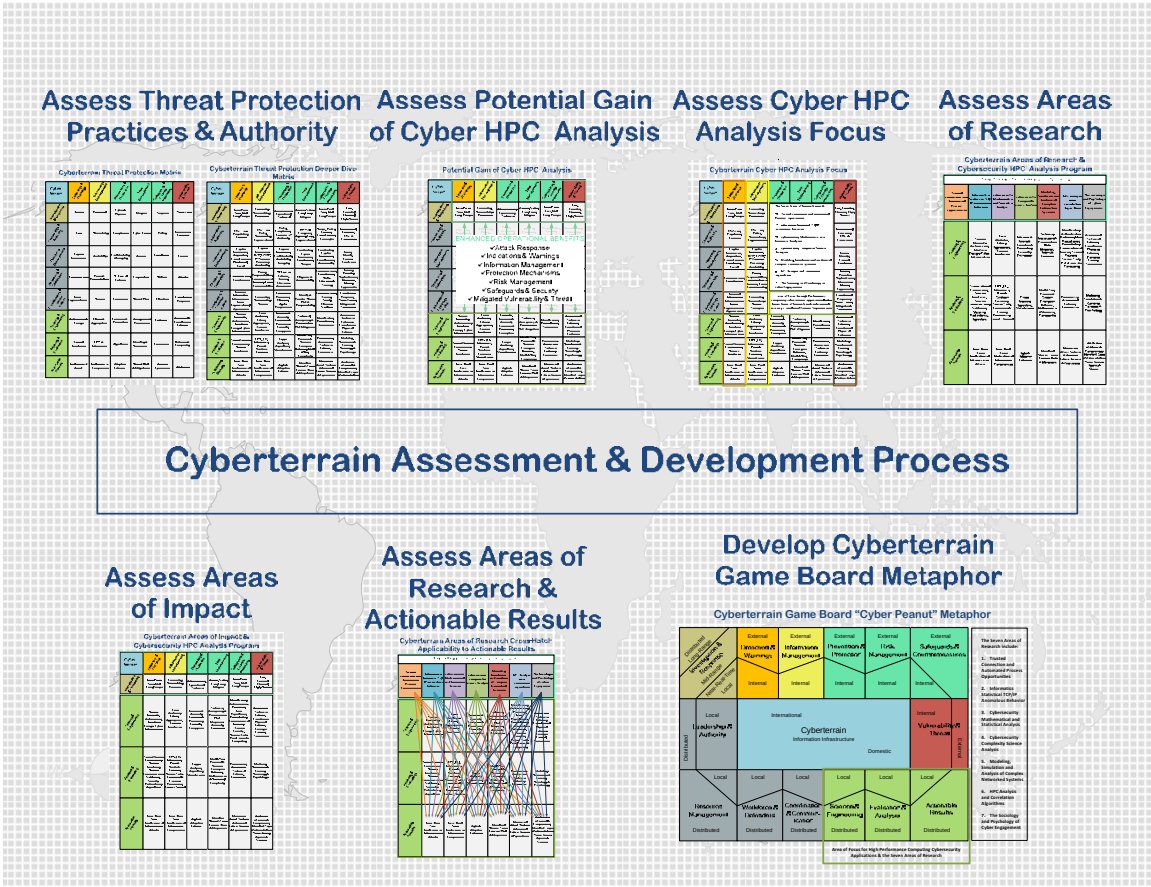


**Figure 1. Cyberterrain Assessment & Game Board Metaphor Development Process**

The fourteen areas or domains of concern were developed after careful consideration of the activities and authorities comprised in securing wide-area national information infrastructure. Figure 2 illustrates the concerns, responsibilities and practices of the cyberterrain created during a mapping/brainstorming exercise. This initial concept and planning exercise illustrated the need for a means of faster time-to-resolution for wide-area "shared" cybersecurity problems, and subsequent national cyber defense solutions. Such solutions would ideally be graded to the level of threat and the value of information assets at risk.

What is being done is not enough as evidenced by an escalating global cyber threat. Capital investments are needed to underwrite improved function and efficiency in each of the domains of concern. Key to a strengthened national cybersecurity posture is an increased and continued investment in advanced capability development, such as HPC analysis, and continued national leadership for broad coordination and communication.

**Cyberterrain Threat Protection Deeper Dive Matrix**

| Cyber-terrain | Detection & Warnings | Information Management | Prevention & Protection | Risk Management | Safeguards & Counter-measures | Vulnerability & Threat |
|---|---|---|---|---|---|---|
| Investigation & Response | Near-Real-Time, Mid-Long-Range | Ownership, Stewardship, Protection | Administrative, Operational, Technical | Assess, Value, Cost, Loss, Mitigate | Near-Real-Time, Mid-Long-Range | Low, Guarded, Elevated, High, Severe |
| Leadership & Authority | USG Law, Regulation, Domain | USG Law, Policy, Stewardship, Organizational | Policy, Compliance, Domains of Authority | POTUS, Congress, Agency, Dept., Organizational | Scope, Policy, Domain, Cross-Domain, Oversight | International, Domestic, USG & Commercial |
| Resource Management | Capital Investment, Acquisition, Cross-Domain Distributed, Local | Capital Investment, BCP, COOP, IT Disaster Recovery, Availability | Capital Investment, Confidentiality, Availability, Integrity | Leadership, Capital Investment, Coordination, Scope | Leadership, Capital Investment, Coordination, Actionability | Invest, Identify, Control, Eradicate |
| Workforce & Defenders | Communication, Coordination | Roles, Responsibilities, Communities of Interest, Data Discoverability | 1st Line of Defense, Training, Education, Awareness | Diligence & Accountability | Communication, Coordination, Skills, Education & Training | Insider, Outsider, Sophistication, Motivation, Means, Opportunity |
| Coordination & Commun-ication | National Information Infrastructure Inter-Organizational, Agreements | Ownership, Stewardship, Secure | Consistent Protection, Effective, Agile, Responsive | Identify & Resolve Shared Risk & Responsibility | Communication, Training, Timely, Effective, Verified | Coordinated Response, Threat Levels, Mitigation & Termination |
| Science & Engineering | Sensor Networks, Architectures, Interface Design, Cyber-Infrastructure | Data Attributes, Filters, Aggregation, Trusted Interfaces | Intrusion & Anomaly Detection & Prevention, Firewalls, Encryption | Technical, Anticipatory & Preventative Risk Mitigation | Identification, Remediation, Termination | Automated Technical Defense, Coordinated Physical Defense |
| Analysis & Evaluation | Trusted Internet Connections, Secure Interfaces | HPC, I/O, Informatics, Real & Synthetic Datasets | Crypt-Analysis, Algorithms, Virtualization | Mod & Sim, Protocol & System Emergent Behavior, Math & Stat, Complexity | Provenance, Automated Technical Defense, Deterrence | Modeling, Simulation & Gaming, Sociology & Psychology |
| Actionable Results | Near Real Time Notification of Infrastructure Attack | Near Real Time Notification of Information Compromise | Agile & Adaptive Defense | Identified Shared Cross Domain Risk & Mitigations | Minimized Attack Surface & Assured Critical Access & Operations | Attribution of Attack & Compromise, Identified Gaps & Vulnerabilities |

**Figure 2. Cybersecurity Subject Matter Matrix**

The full game board includes cybersecurity domains of concern (illustrated in bold type in Figure 3.). The "Internal" and "External" boundary represents the border between the national information infrastructure and the world-wide Internet. Similarly, the "Local" versus "Distributed" boundary represents the scope of authority and/or collaboration for wide-area interconnected autonomous area networks, information systems, and cyber-infrastructure. Note the "Cyber Peanut" form taken from the shape of the internal/external and local/distributed borders that is representative of a continuous cyberterrain lifecycle, which includes human, organizational, legal and technical interdependencies.

Note that the Detection and Warnings domain, as opposed to Indications and Warnings, is referenced to better define this domain in terms of cybersecurity practices within the cyberterrain. Also illustrated in figure 3 are the seven areas of recommended HPC research that were identified in the assessment of the CIWD and the HPC cybersecurity application area of focus comprising the Science and Engineering, Evaluation and Analysis, and Actionable Results domains of concern.

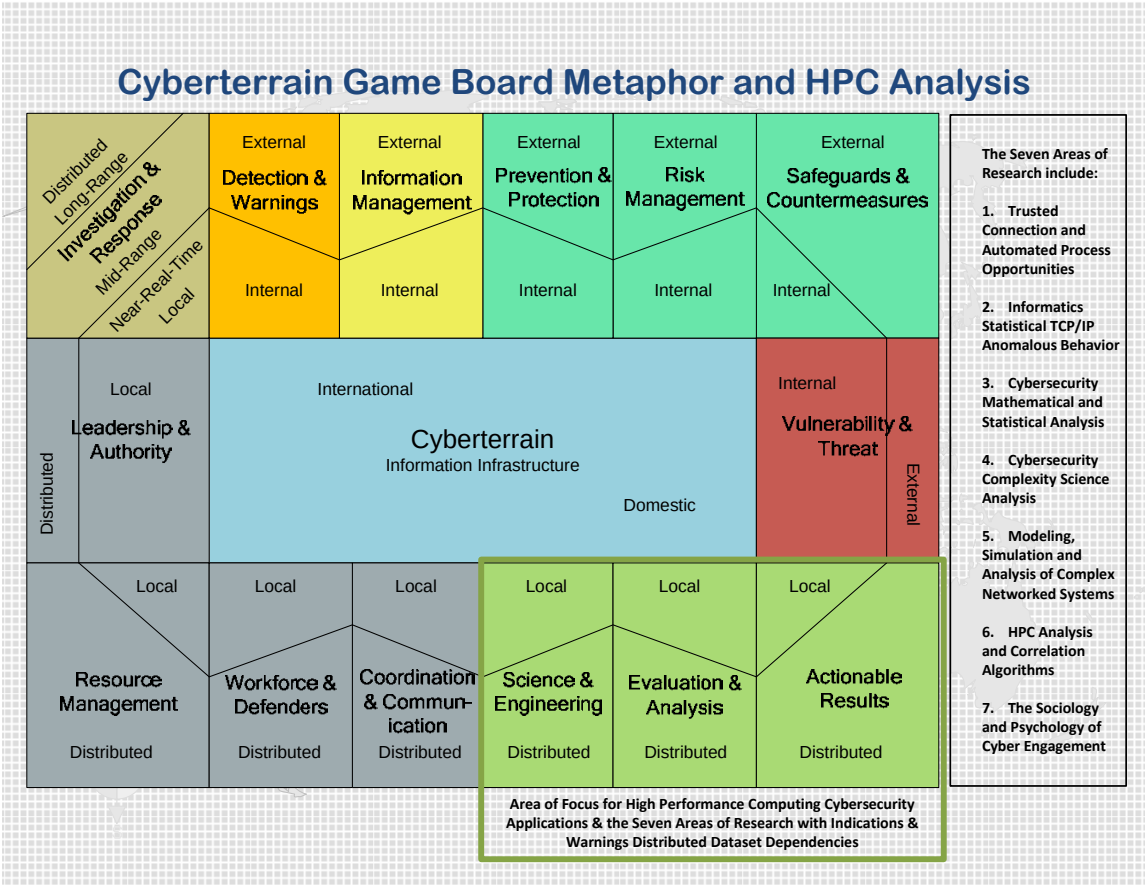


**Figure 3. Cyberterrain Game Board and Advanced Cyber HPC Analysis Area of Focus**

Each domain of concern in the cyberterrain problem space is broad in scope and each comprises diverse aspects and disciplines. The cyberterrain domains of concern are:

1. Threat & Vulnerability
2. Safeguards and Countermeasures
3. Risk Management
4. Prevention and Protection
5. Information Management
6. Detection and Warnings
7. Investigation and Response
8. Leadership and Authority
9. Resource Requirements
10. Workforce and Defenders
11. Coordination and Communication
12. Science and Engineering
13. Evaluation and Analysis
14. Actionable Results

Cyberterrain defense can be expressed as a continuum that establishes translation through an accompanying nomenclature. The nomenclature continuum permits consistent expression and execution as cyber defense initiatives move from one view to the next while accommodating view specific syntax.

Each view uses appropriate language and terminology for view specific purpose. For example, the operational view uses business specific terms. Notice that representation is domain of concern and goal oriented as opposed to technical jargon.

**Table 1. Cyberterrain Defense and Nomenclature Continuums**

| **CYBERTERRAIN DEFENSE CONTINUUM ↔** | | | | |
|---|---|---|---|---|
| **Executive View** | **Operational View** | **Risk View** | **Protection View** | **Defense View** |
| Leadership and Authority, Coordination and Communication | Information Management, Resource Management, Work Force and Defenders, Coordination and Communication | Vulnerability and Threat, Risk Management | Safeguards and Countermeasures, Prevention and Protection | Science and Technology, Evaluation and Analysis, Actionable Results, Detection and Warnings, Investigation and Response |
| Inform the Decision Maker | Inform the Defender | Minimize Exposure | Reduce the Attack Surface | Effective Defense |
| **NOMENCLATURE CONTINUUM ↔** | | | | |

Network and information technology environments are intricate and complex. Therefore the cyber terrain continuum views are expressed in terms of a variety of perspectives.

Consider a *business perspective* for example: organizational relationships; contract and legal liabilities; operational dependencies; inter-organizational process requirements; and business continuity requirements comprise a business to business perspective.

Consider a *system of systems perspective* for example: distributed computational capabilities and capacity and system interfaces comprise an interconnected systems perspective; I/O characterization of data types, transactional data exchange and throughput or time requirements comprise an I/O perspective; service level agreement requirements comprise a telecommunications service perspective.

Consider a *user perspective* for example: stakeholders, data owners and data stewards, and all manner of consumers of information that generate, process, review and otherwise access information comprise a user perspective.

Consider a *component/device perspective* for example: Internet enabled cell phones and personal digital assistants (PDA), home computing, web interface, data storage servers and client hosts comprise a user component perspective; routing and switching telecommunications equipment comprise a telecommunication provider component perspective.

Consider an *operational support systems (OSS) perspective* for example: maintenance and operations include systems for monitoring heartbeat (host availability) and health (service availability), and datacenter environmental controls (HVAC and power). An OSS perspective represents business continuity concerns and indirect attack surfaces.

Consider an *application perspective* for example: order entry, email and messaging services such as twitter comprise a user application perspective; database, automated job processing and data backup comprise an operational application perspective; log review and auditing comprise a security application perspective.

Consider a *service perspective* for example: web based entertainment and online gaming, online banking, and public information access comprise a user or consumer services perspective; authentication services such as lightweight directory access protocol (LDAP) and Kerberos (authentication ticket), and intrusion detection and prevention comprise a security service perspective; the Domain Name Service (DNS) name resolution to IP address, network time protocol (NTP), dynamic host configuration protocol (DHCP) comprise a network services perspective. Middleware and data synchronization comprise an operational service perspective. Service disruption and denial of service represent a common attack vector.

Consider a *function perspective* for example: manufacturing, packaging, shipping and distribution of goods and services comprise a supply chain function perspective; consumer trends, supply and demand, and materials availability comprise a product delivery function perspective; asset valuation, funds availability and liabilities, and procurement comprise a financial function perspective. Interruption of supply chain, product delivery or financial means

of operation represent ancillary human or natural disaster threat vectors that impact continuity of operations.

Consider an *information asset perspective* for example: publically available information comprise a sharable information asset perspective; categorization such as mandatory labeling for classification of data such as confidential and secret, and intellectual property such as proprietary information and trade secrets comprise a sensitive information asset perspective; health records information comprise a private information asset perspective; and public safety records comprise a need-to-share information asset perspective. Taxonomy of information assets may reveal that some information is of such a value that it would better be destroyed than released.

Consider an *information access perspective* for example: communities of interest (COI) comprise a consumer information access perspective; creation and disposition of information comprise a data owner information access perspective; processing and handling of information comprise a data steward need-to-know information access perspective; local and remote access comprise a locality information access perspective; and finally an inappropriate use or modification of information comprise a *no information access* perspective.

Consider an *adversary perspective* for example: generic threat profiles comprise an adversarial capability perspective [5] [SAND2005-5411]. The following is an excerpt from the Generic Threat Profiles Sandia report that describes an adversarial threat in terms of capability, which avoids the use of ambivalent terms such as "Nation State". Expression of adversarial threat as a capability provides the benefit of model reuse for simulating various threat scenarios.

"Threat profiles are a way to bin threat organizations of differing political, social, and motivation structures such that relevant characteristics may be utilized in identifying classes of attacks each might be able to carry out."

**Table 2. Threat Characteristics**

| Category | Funding | Goal Intensity | Stealth | Physical Access | Cyber Skills | Implementation Time | Cyber Org Size |
|---|---|---|---|---|---|---|---|
| **I** | H | H | H | H | H | Decades/Years | Hundreds |
| **II** | H | H | H | M | M | Years | Tens of Tens |
| **III** | M | H | M | M | M | Months | Tens |
| **IV** | L | M | H | L | H | Months | Tens |
| **V** | L | M | M | L | M | Months | Ones |
| **VI** | L | L | L | L | L | Weeks | One |

[5] SAND2005-5411, Generic Threat Profiles, David P. Duggan, Unlimited Release, July, 2005

### *3.1.1 Cyberterrain Problem Space: Assessment Conclusions*

1. The tie between HPC and the cyberterrain game board is that advanced HPC analysis for cybersecurity is founded in the areas of science and engineering, evaluation and analysis, and actionable results that could have potentially profound impact in the Cyberterrain.

2. Cybersecurity HPC analysis is a potentially game changing means to support a wide-area rapid time-to-solution national cyber defense capability.

3. Key to a strengthened national cybersecurity posture is an increased and continued investment in science and technology advanced capability development, such as HPC analysis, and continued national leadership for broad coordination and communication.

4. Cyber defense can be expressed as a continuum with an accompanying nomenclature continuum to facilitate multi-organizational communication toward common wide-area cybersecurity goals.

5. The cyberterrain continuum views should be further defined and expressed in terms of a variety of perspectives to capture complexity.

## 3.2 Areas of Impact, Priority Problems, Research, and Actionable Results

*Goal: Develop actionable results with regard to priority problems and promising areas of research that are applicable to wide-area national cyber defense.*

The cyberterrain areas of concern pertaining to this phase of assessment are:

1. Threat & Vulnerability
2. Safeguards and Countermeasures
3. Risk Management
4. Prevention and Protection
5. Information Management
6. Detection and Warnings
7. Investigation and Response
8. Science and Engineering
9. Evaluation and Analysis
10. Actionable Results

Specific areas of impact were identified that are significant in that a more robust and resilient wide-area protection posture can be achieved through applied science and technology, evaluation and analysis, and actionable results made possible with cybersecurity HPC analysis. Consider that the wide-area comprises technical, organizational and human complexity on a grand scale and dependency on this system of systems results in the need for sustainable confidentiality,

integrity and availability of immense volumes of data. Therefore, an investment in HPC analysis aligned with national cyber defense will need to meet this scale of economy.

Areas of impact include:

1. Threat & Vulnerability
2. Safeguards and Countermeasures
3. Risk Management
4. Prevention and Protection
5. Information Management
6. Detection and Warnings
7. Investigation and Response

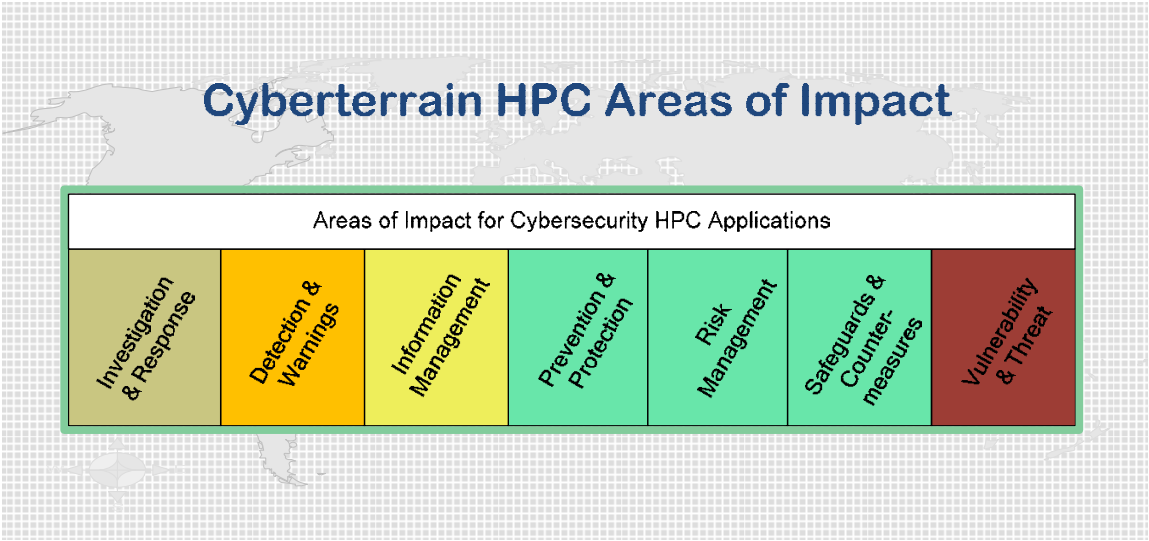


**Figure 4: Cyberterrain Areas of Impact**

An industry surrounding computer network defense (CND) has developed to address the threat of computer network attack (CNA) and exploitation (CNE). Common vulnerabilities and exposures (CVE) are widely present and exploited across all main stream computing platforms, information services and telecommunication protocols. The following priority wide-area cybersecurity problems are considered in a broad context to include multiple autonomous areas of responsibility, varied technological investments and priorities, and increased shared risk due to local cyber-defense planning and implementation without efficient consideration for the common system-of-systems infrastructure. It is at this level of shared risk that the priority wide-area cybersecurity problems align with the cyberterrain areas of impact.

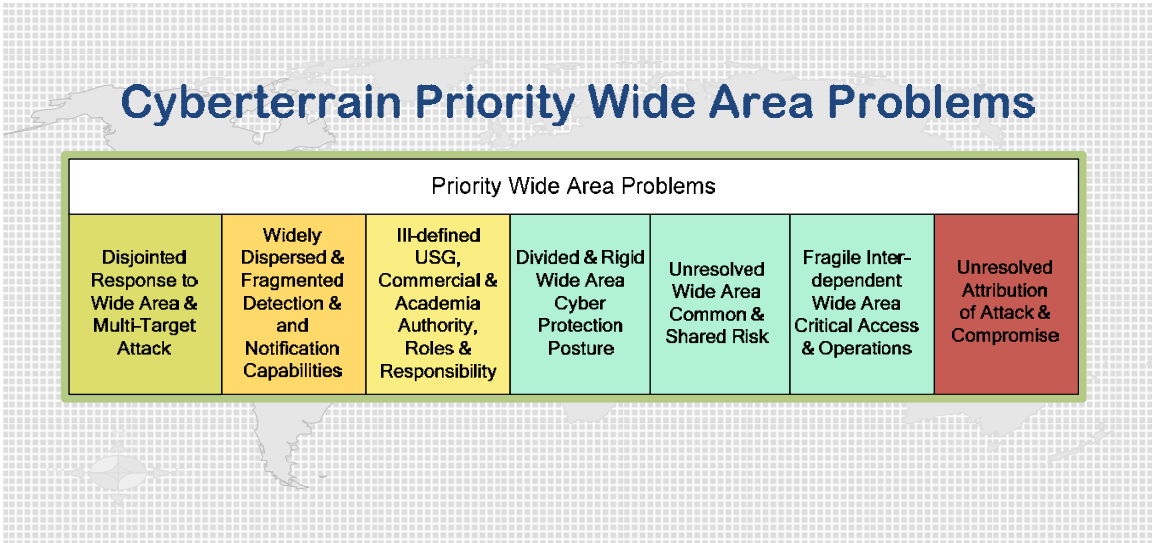


**Figure 5: Cyberterrain Priority Wide-Area Problems**

The most pressing of these problems is unresolved attribution of attack and compromise. Without confidence in the attribution of attack an effective response is difficult to mount against the responsible adversary. Furthermore, cyber deterrence is ineffective without a means to identify the level of sophistication and who is responsible for attack. Action can only be taken when malicious incursion can be readily attributed to the responsible party.

Science, technology, evaluation and analysis form the basis of HPC cybersecurity research applications with the purpose of producing actionable results for an improved wide-area protection posture. The HPC analysis areas of research are broadly applicable in the cyberterrain and have anticipated far reaching results to national cyber defense.

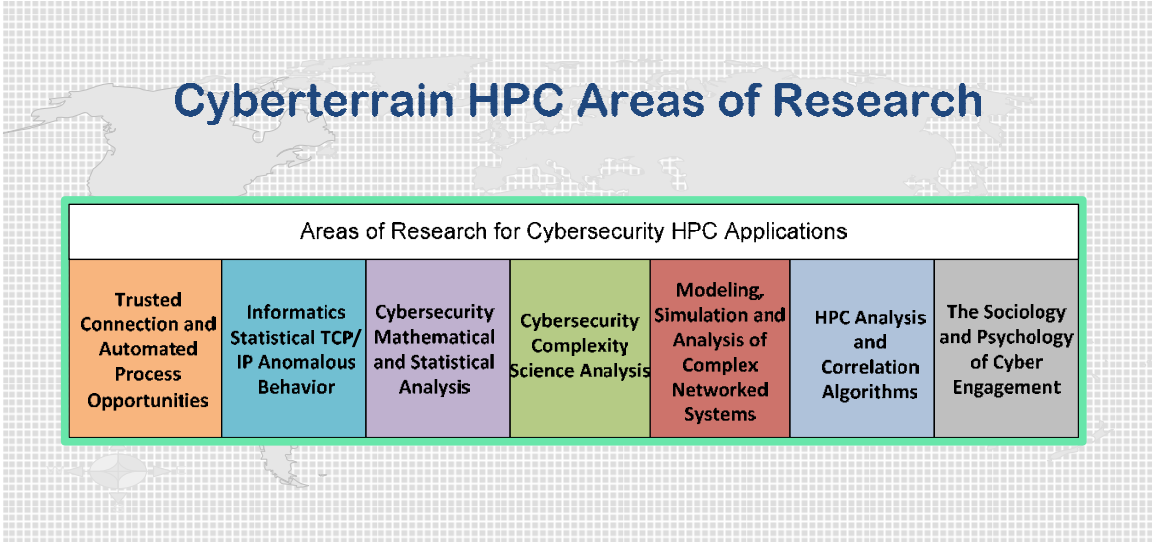


**Figure 6: Cyberterrain HPC Analysis Areas of Research**

A fuller description of the recommended areas of research for HPC Cybersecurity applications is provided below.

1. Identify Trusted Connections and Automated Process Opportunities for Collecting and Analyzing Information for Cybersecurity Applications.

2. Examine Informatics Statistical TCP/IP Anomalous Behavior Research for protocol anomalous and malicious characteristics; analysis of temporal and spatial characteristics of attack; harvesting data to seed Informatics visual analytics for cybersecurity subject matter.

3. Examine Cybersecurity Mathematical and Statistical Analysis Research to collect, handle, and analyze large datasets for modeling, intrusion detection, attack response, and identification of multistage attacks.

4. Examine Cybersecurity Complexity Science Analysis Research for studying the unpredictability in programs, machines, and networks, and large-scale modeling and simulation.

5. Examine Modeling, Simulation and Analysis of Complex Networked Systems, including large scale network models and models of network dynamics and cyber attack. Applications include intrusion detection, and examining the evolution of cyber threats.

6. Expand HPC Analysis and Correlation Algorithms for identification of temporal and spatial characteristics associated with anomalous events, and detection of widespread, multistage, multiple method attacks.

7. Understand the Sociology and Psychology of Cyber Engagement for solving the problem of attributing an attack to responsible parties, and to aid in the development of anticipatory and preventative safeguards and countermeasures based on predictable behaviors.

8. Potential benefits of HPC cybersecurity research include the study and understanding of emergent behavior, anomalous and malicious characteristics, and the modeling and simulation of complex systems that is beyond human comprehension without the utility of supercomputing. Human directive and interaction can also be analyzed and understood through study of the psychology and sociology of attacker/defender behavior with potential advancement of predictive and anticipatory cyber defense technologies. Such complex and data intensive studies are not feasible without HPC cybersecurity analysis.

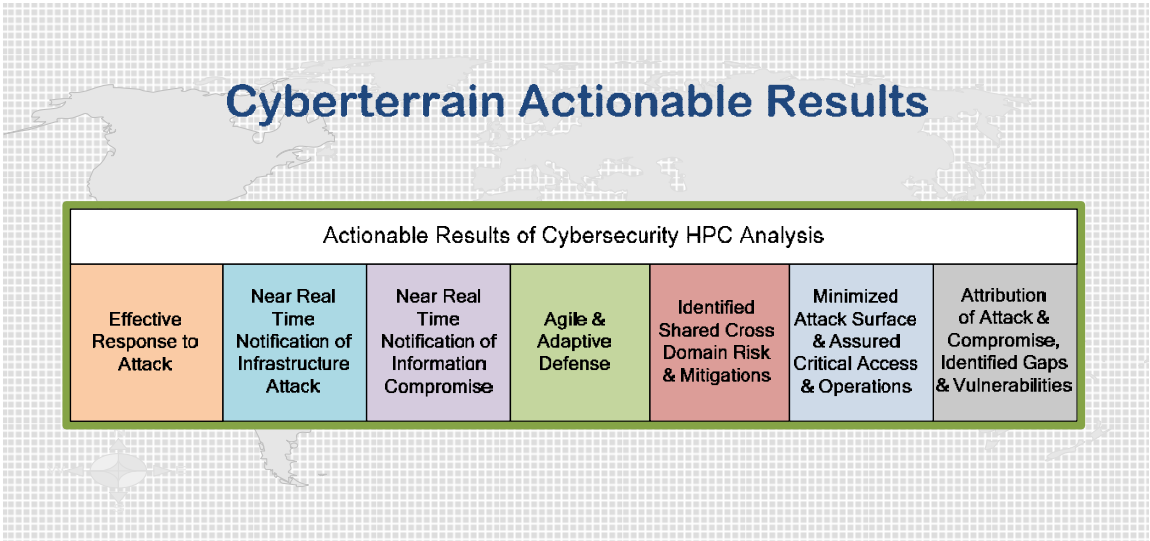


**Figure 7: Targeted Actionable Results of Cybersecurity HPC Analysis**

The proposed actionable results are broad in scope and are closely aligned with priority wide-area problems. Evaluation and analysis are expected to lead to greater understanding of development for a strengthened national cyber defense capability. This assessment finds a growing foundation of cybersecurity research and development, although limited funds availability and a lack of multi-agency program support threaten continued viability.

The actionable results listed below are considered as shared goals to facilitate a more secure national information infrastructure.

1. Identification of Gaps and Vulnerabilities
2. Effective Response to Attack
3. Near Real-Time Notification of Infrastructure Attack and Information compromise
4. Agile and Adaptive Defense
5. Identified Cross Domain Risks and Mitigations
6. Minimized Attack Surface
7. Assured Critical Access and Operations
8. Attribution of Attack and Compromise

Critically important to national cyber defense is the coordination required to identify shared risks, gaps and vulnerabilities, without which an effective response to wide-area or sophisticated multi-stage cyber attacks is insurmountable. Resolution of conflicts of interest in the protection of intellectual property, mission overlap, and competition for funding and authority within government is needed for improved coordination. Coordination is further inhibited by a lack of established and commonly understood roles and responsibilities for the handling and management of cyber threat data across organizations.

Areas of Impact, Priority Problems, Areas of Research, Actionable Results: Assessment Conclusions

1. An investment in HPC analysis areas of research aligned with cyber defense areas of impact and priority problems is essential for continued progress toward a national cyber defense capability.

2. Cyber deterrence is ineffective without a means to identify the level of sophistication and who is responsible for attack.

3. The study and understanding of technical, organizational and human complexity within the wide-area national information infrastructure is beyond human comprehension without the utility of supercomputing.

4. Ongoing work indicates a growing foundation of HPC cybersecurity research and development, although limited funds availability and lack of multi-agency program support threaten continued viability.

5. Critically important to national cyber defense is the coordination and work toward shared goals to address shared risks and therefore an effective defense to wide-area or sophisticated multi-stage attack.

## 3.3 Fundamental Relationships, Integration and Potential Benefits

*Goal: Develop an understanding of fundamental relationships and integration, customer objectives, application, function, conceptual gains, realization, and potential benefit.*

The cyberterrain areas of concern pertaining to this phase of assessment are:

1. Threat & Vulnerability
2. Safeguards and Countermeasures
3. Risk Management
4. Prevention and Protection
5. Information Management
6. Detection and Warnings
7. Investigation and Response
8. Science and Engineering
9. Evaluation and Analysis
10. Actionable Results

This phase of the planning exercise was conducted to develop an understanding of fundamental relationships and integration. Our approach considered customer objectives, application, function, conceptual gain (near and long term), and realization (CAFCR)[6]. Integrating elements, integrating principles and threads of reasoning were considered for high-value areas of impact

[6] References taken from Architectural Reasoning Explained, Gettit Muller, 2010, http://www.gaudisite.nl

and priority wide-area problems. Similarly, Integrating elements, principles and threads of reasoning were considered for high-value areas of research, and actionable results.

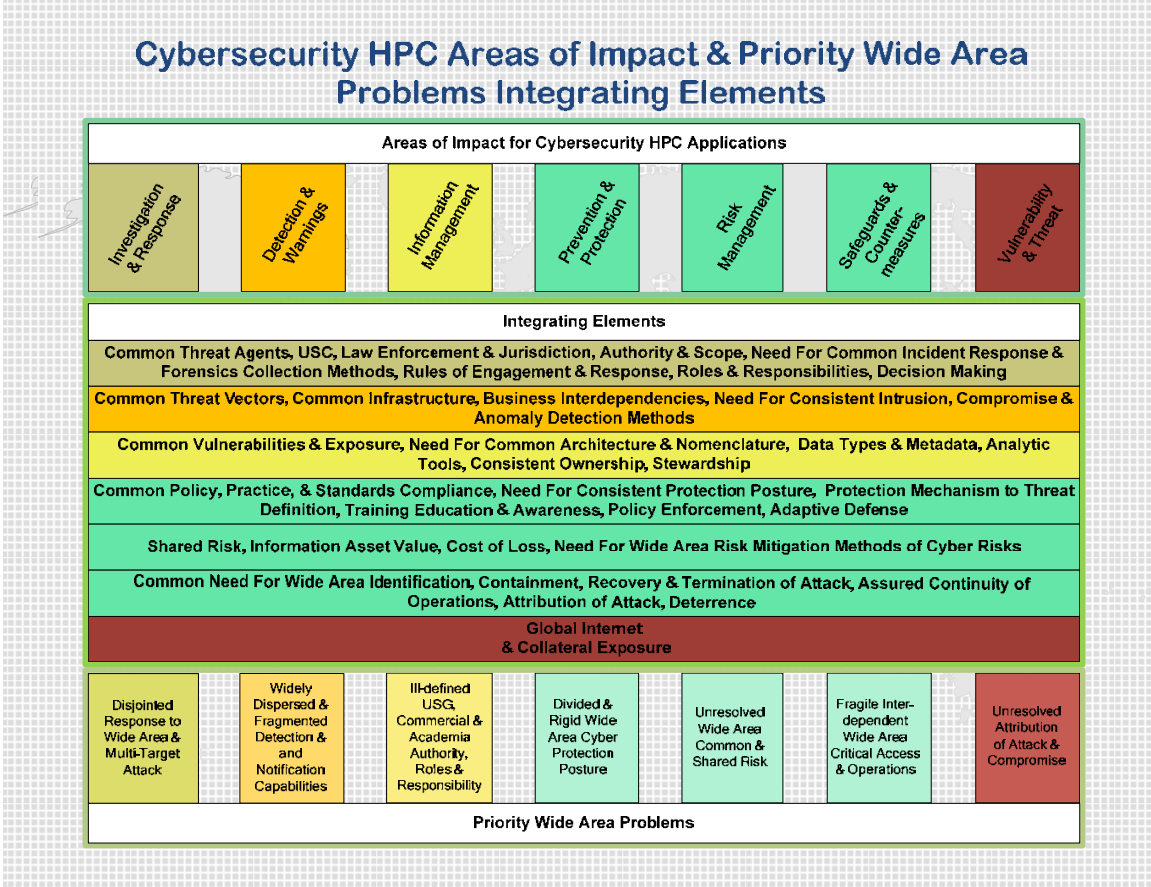


**Figure 8: Areas of Impact, Priority Problems & Integrating Elements**

Illustrated in figures 8 and 9 are thumbnail assessments of fundamental relationships and integration for each area of impact to a specific wide area priority problem. In figure 8 consider that integrating elements span the spectrum of political, inter-organizational, guidance and practice, and geographic and technical lifecycles in the cyberterrain.

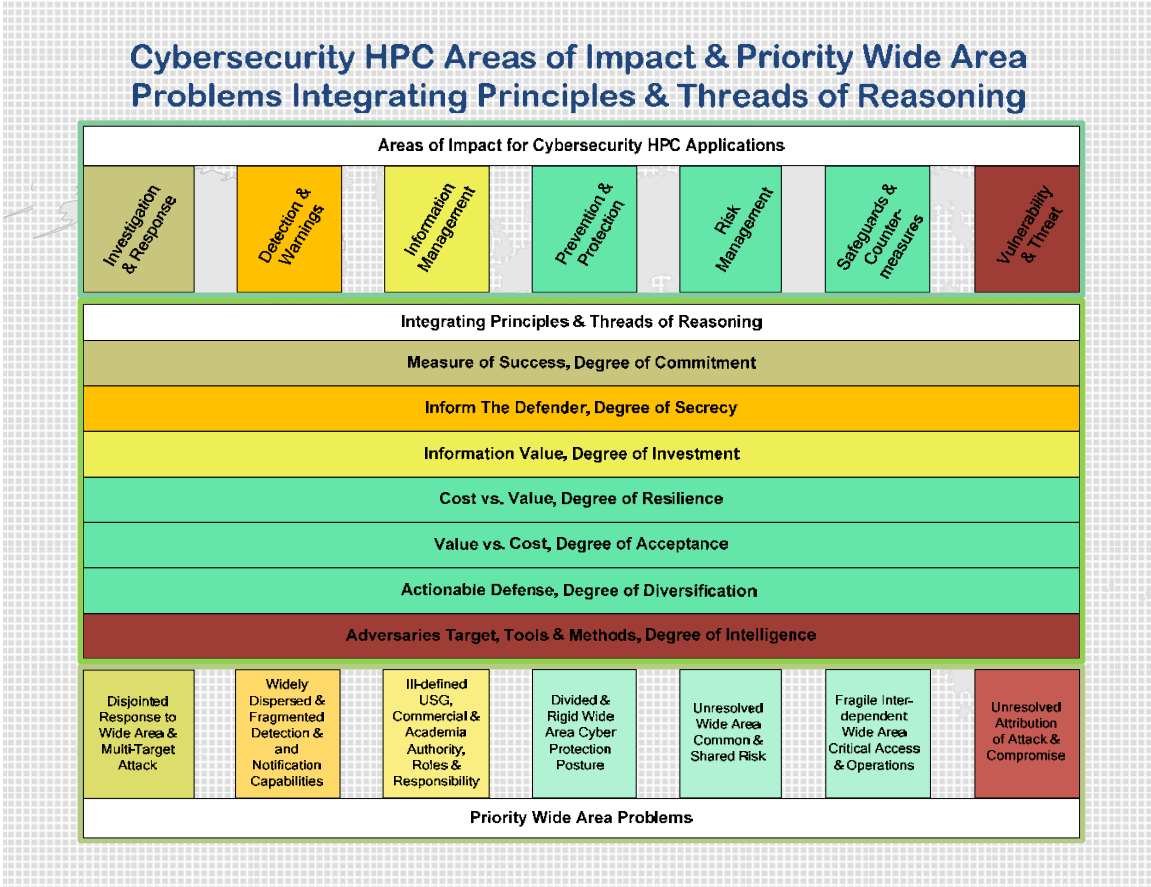


**Figure 9: Areas of Impact, Priority Problems, Integrating Principles & Threads of Reasoning**

Integrating elements, principles, and threads of reasoning were enumerated as being rooted in one area of impact and affecting the other areas of impact in the same way that protection posture and information management practices affect preparedness.

What is intended is a representation of a holistic balanced national cyber defense capability with quantified goals in a progressive approach to a comprehensive set of solutions. Fundamental to this approach is the integral relationship of function and security as opposed to function vs. security.

**Investigation and Response Domain of Concern**

*Priority Wide Area Problem*: Disjointed Response to Wide Area & Multi-Target Attack

*Integrating elements of investigation and response as a high-value area of impact*:
Common Threat Agents; USC, Law Enforcement and Jurisdiction; Authority and Scope; Need for Common Incident Response and Forensics Collection Methods, Rules of Engagement and Response, Defined Roles and Responsibilities, and Informed Decision Making

*Integrating principles and threads of reasoning for investigation and response as a high-value area of impact*: Measure of Success; Degree of Commitment

**Detection and Warnings Domain of Concern**
*Priority Wide Area Problem*: Widely Dispersed and Fragmented Detection and Notification Capabilities

*Integrating elements of detection and warnings as a high-value area of impact*:
Common Threat Vectors; Common Infrastructure; Business Interdependencies; Need for Consistent Intrusion, Compromise and Anomaly Detection Methods

*Integrating principles and threads of reasoning for detection and warnings as a high-value area of impact*: Inform the Defender; Degree of Secrecy

**Information Management Domain of Concern**
*Priority Wide Area Problem*: Ill-defined USG, Commercial & Academia Authority, Roles & Responsibility

*Integrating elements of information management as a high-value area of impact*:
Common Vulnerabilities and Exposure; Need for Common Architecture and Nomenclature, Defined Data Types and Metadata, Analytic Tools, and Consistent Ownership and Stewardship

*Integrating principles and threads of reasoning for information management as a high-value area of impact*: Information Value; Degree of Investment

**Prevention and Protection Domain of Concern**
*Priority Wide Area Problem*: Divided and Rigid Wide Area Cyber Protection Posture

*Integrating elements of prevention and protection as a high-value area of impact*:
Common Policy, Practice, and Standards Compliance; Need for Consistent Protection Posture, Protection Mechanism to Threat Definition, Training Education and Awareness, Policy Enforcement, and Adaptive Defense

*Integrating principles and threads of reasoning for prevention and protection as a high-value area of impact*: Cost vs. Value; Degree of Resilience

**Risk Management Domain of Concern**
*Priority Wide Area Problem*: Unresolved Wide Area Common and Shared Risk

*Integrating elements of risk management as a high-value area of impact*:
Shared Risk, Information Asset Value, Cost of Loss; Need for Risk Mitigation Methods of Wide-Area Cyber Risks

Integrating principles and threads of reasoning for risk management as a high-value area of impact: Value vs. Cost; Degree of Acceptance

**Safeguards and Countermeasures Domain of Concern**
Priority Wide Area Problem: Fragile Interdependent Wide Area Critical Access and Operations

Integrating elements of safeguards and countermeasures as a high-value area of impact:
Need for Wide Area Identification, Containment, Recovery and Termination of Attack, Assured Continuity of Operations, Attribution of Attack, and Deterrence

Integrating principles and threads of reasoning for safeguards and countermeasures as a high-value area of impact: Actionable Defense; Degree of Diversification

**Vulnerability and Threat Domain of Concern**
Priority Wide Area Problem: Unresolved Attribution of Attack and Compromise

Integrating elements of vulnerability and threat as a high-value area of impact:
Global Internet and Collateral Exposure

Integrating principles and threads of reasoning for vulnerability and threat as a high-value area of impact: Adversaries Target, Tools and Methods; Degree of Intelligence

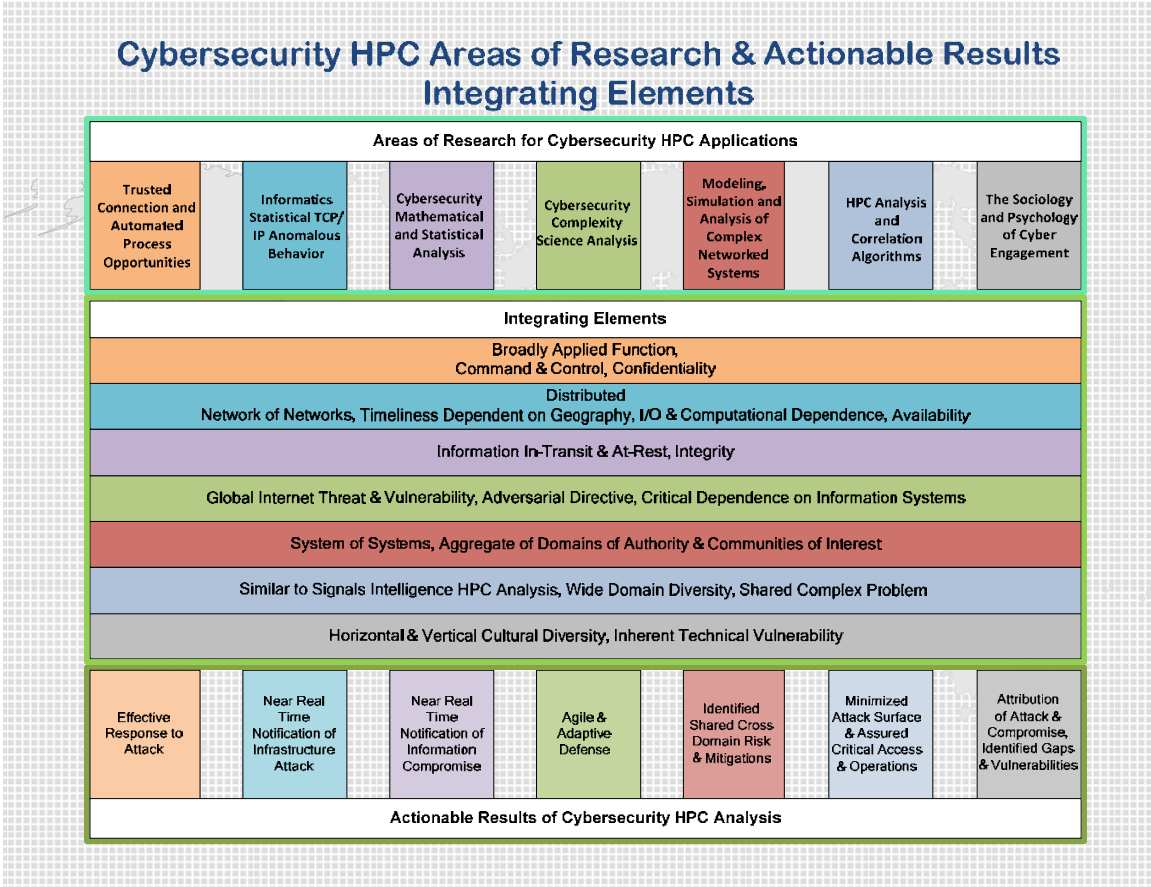


**Figure 10: Areas of Research, Actionable Results & Integrating Elements**

Illustrated in figures 10 and 11 are thumbnail assessments of fundamental relationships and integration for each area of research to a related wide area actionable result.

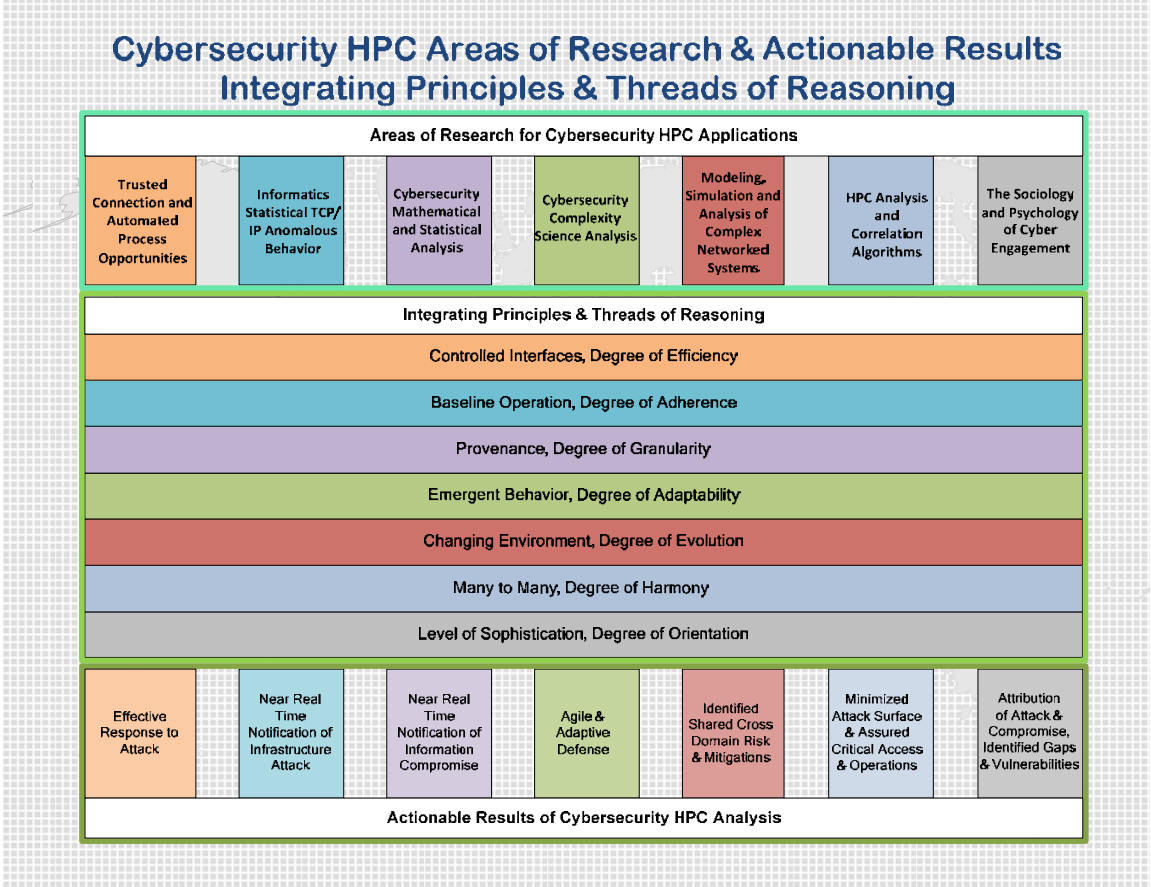


**Figure 11: Areas of Research, Actionable Results, Integrating Principles & Threads of Reasoning**

**Trusted Connection and Automated Process Opportunities Area of Research**
*Actionable Result:* Effective Response to Attack

*Integrating elements of trusted connection and automated process opportunities as a high-value area of research*: Broadly Applied Function, Command and Control, and Confidentiality

*Integrating principles and threads of reasoning for trusted connection and automated process opportunities as a high-value area of research*: Controlled Interfaces; Degree of Efficiency

**Informatics Statistical TCP/IP Anomalous Behavior Area of Research**
*Actionable Result:* Near Real Time Notification of Infrastructure Attack

*Integrating elements of informatics statistical TCP/IP anomalous behavior as a high-value area of research*: Distributed Network of Networks, Timeliness Dependent on Geography, I/O and Computational Dependence, Availability

*Integrating principles and threads of reasoning for statistical TCP/IP anomalous behavior as a high-value area of research*: Baseline Operation; Degree of Adherence

**Cybersecurity Mathematical and Statistical Analysis Area of Research**
*Actionable Result:* Near Real Time Notification of Information Compromise

*Integrating elements of cybersecurity mathematical and statistical analysis as a high-value area of research*: Information In-Transit and At-Rest; Integrity

*Integrating principles and threads of reasoning for* cybersecurity mathematical and statistical analysis *as a high-value area of research*: Provenance; Degree of Granularity

**Cybersecurity Complexity Science Analysis Area of Research**
*Actionable Result:* Agile & Adaptive Defense

*Integrating elements of cybersecurity complexity science analysis as a high-value area of research*: Global Internet Threat and Vulnerability, Adversarial Directive, Critical Dependence on Information Systems

*Integrating principles and threads of reasoning for cybersecurity complexity science analysis as a high-value area of research*: Emergent Behavior; Degree of Adaptability

**Modeling, Simulation and Analysis of Complex Networked Systems Area of Research**
*Actionable Result:* Identified Shared Cross Domain Risk and Mitigations

*Integrating elements of modeling, simulation and analysis of complex networked systems as a high-value area of research*: System of Systems, Aggregate of Domains of Authority and Communities of Interest

*Integrating principles and threads of reasoning for modeling, simulation and analysis of complex networked systems as a high-value area of research*: Changing Environment; Degree of Evolution

**HPC Analysis and Correlation Algorithms Area of Research**
*Actionable Result:* Minimized Attack Surface and Assured Critical Access and Operations

*Integrating elements of HPC analysis and correlation algorithms as a high-value area of research*: Similar to Signals Intelligence HPC Analysis, Wide Domain Diversity, and Shared Complex Problem

*Integrating principles and threads of reasoning for HPC analysis and correlation algorithms as a high-value area of research*: Many to Many; Degree of Harmony

**The Sociology and Psychology of Cyber Engagement Area of Research**
*Actionable Result:* Attribution of Attack & Compromise, Identified Gaps and Vulnerabilities

*Integrating elements of the sociology and psychology of cyber engagement as a high-value area of research:* Horizontal and Vertical Cultural Diversity, Inherent Technical Vulnerability

*Integrating principles and threads of reasoning for the sociology and psychology of cyber engagement as a high-value area of research*: Level of Sophistication; Degree of Orientation

This assessment of fundamental relationships and integrating aspects is subjective, although it offers insight into the objectives, application, function, concept and realization of a more robust and resilient national information infrastructure.

In the conceptual cyberterrain CAFCR architectural model depicted in figure 12, the customer objectives are representative of the cybersecurity centric areas of concern: investigation and response; detection and warnings; information management; prevention and protection; risk management; safeguards and countermeasures; and threat and vulnerability. The application segment is representative of specific priority problems where improved cyber-defense is needed. The function segment represents goals toward specific areas of improved cybersecurity and defense capability. Conceptual gain is representative of applied near and long term capabilities envisioned as part of holistically secure wide-area information environment. Lastly, the realization segment represents the advancements enabled through HPC cybersecurity application research.

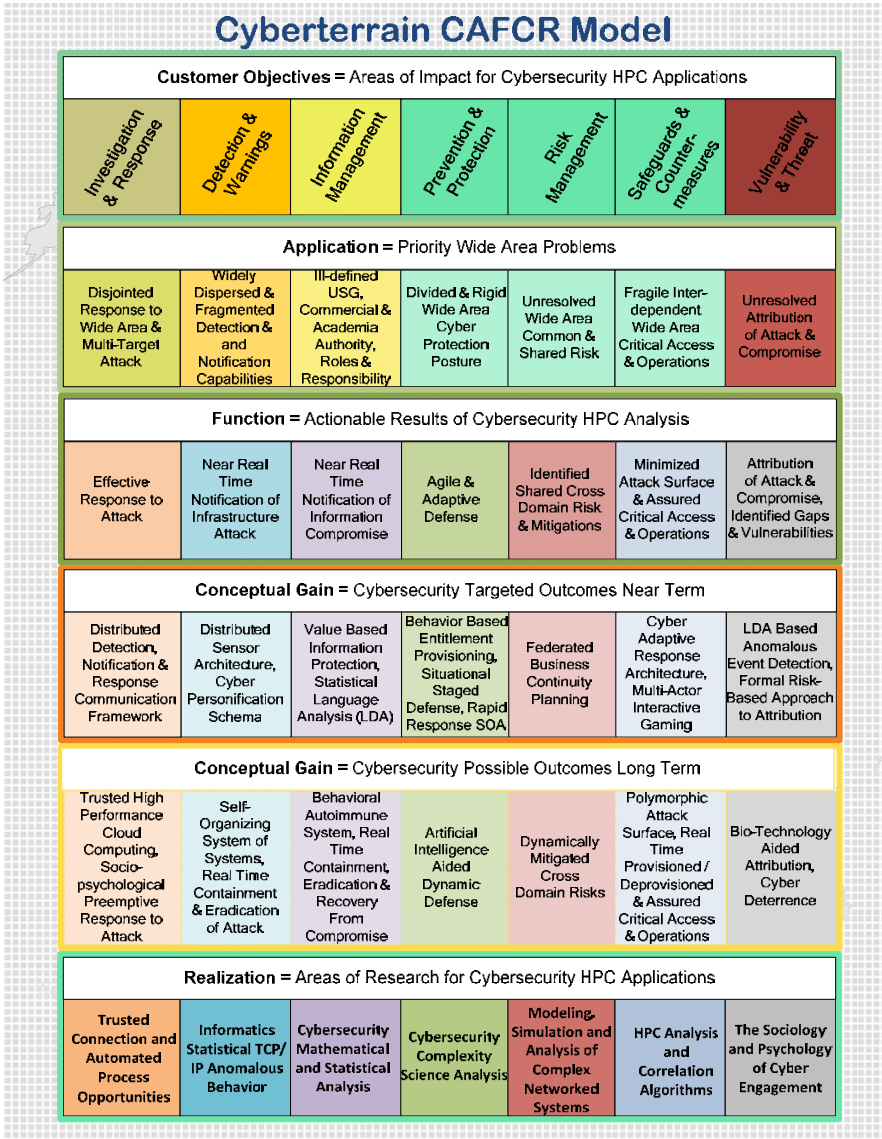


**Figure 12: Customer Objectives, Application, Function, Conceptual & Realization**

Several recent developments with potential high value benefits were identified while conducting an internal review of Sandia National Laboratory activities for the application of HPC for cybersecurity.

1. The National Nuclear Security Administration (NNSA) and Sandia National Laboratories recently dedicated the National Security Computing Center (NSCC). The center is based around the Sandia-built Red Storm supercomputer platform. Its unique capabilities will be applied to help solve pressing national security problems such as cyber defense, vulnerability assessments, informatics (network discovery), space systems threats, and situational awareness.

2. Palacios and Kitten: New High Performance Operating Systems For Scalable Virtualized and Native Supercomputing[7] [Lange, Pedretti, Hudson, Dinda, Cui, Xia, Bridges, Gocke, Jaconette, Levenhagen, and Brightwell]. Palacios is a new high performance virtual machine monitor (VMM) architecture that has been embedded into Kitten, a high performance supercomputing operating system. Together, Palacios and Kitten provide a flexible, high performance virtualized system software platform for HPC systems. This platform broadens the applicability and usability of HPC systems by:

   - providing access to advanced virtualization features such as migration, full system check pointing, and debugging;
   - allowing system owners to support a wider range of applications and to more easily support legacy applications and programming models when changing the underlying hardware platform;
   - enabling system users to incrementally port their codes from small-scale development systems to large-scale supercomputer systems while carefully balancing their performance and system software service requirements with application porting effort; and
   - providing system hardware and software architects with a platform for exploring hardware and system software enhancements without disrupting other applications.

3. Statistical Language Analysis for Automatic Exfiltration Event Detection[8] [SAND2010-2179]. This paper discusses a statistical approach for the automatic identification of anomalous network activity that is characteristic of exfiltration events. This approach is based on the language processing method referred to as latent dirichlet allocation (LDA). Current rule-based systems only apply to exfiltration behavior that has previously been observed. Since the LDA methodology is not a rules based approach, it makes it more difficult for insiders to hide data exfiltration activities. The results of LDA analysis provide a refined dataset of previously unobserved suspect network activity that are identified early (before firewall rules and antivirus signatures can be developed and distributed) for rapid response and investigation. New insights to the science of information analysis are emerging with mathematical techniques associated with probabilistic latent semantic analysis.

These recent advancements are important because they represent current work that provides a foundation for continued advancement of cybersecurity applications and HPC research and analysis. The NSCC is an example of the level of leadership investment needed for advancing HPC analysis for cybersecurity applications.

---

[7] Palacios and Kitten: New High Performance Operating Systems For Scalable Virtualized and Native Supercomputing, John Lange, Kevin Pedretti, Trammell Hudson, Peter Dinda, Zheng Cui, Lei Xia, Patrick Bridges, Andy Gocke, Steven Jaconette, Mike Levenhagen, and Ron Brightwell
Northwestern University, Department of Electrical Engineering and Computer Science
Sandia National Laboratories, Scalable System Software Department
University of New Mexico, Department of Computer Science

[8] SAND2010-2179 Statistical Language Analysis for Automatic Exfiltration Event Detection, April 2010

Palacios and Kitten are representative of the advanced automation (virtualization) of operating systems. Such innovation is also evidenced by commercial virtualization displacing many conventional client server deployments. Palacios and Kitten provide the advantage of scale applicable to HPC platforms. Moreover, modeling and simulation of very large complex systems may lead to reduced cost and time-to-deployment of cyber defense in kind with that of virtualization in the datacenter.

LDA statistical language analysis enables anomaly detection that is a departure from the signature and rules based systems that cybersecurity applications are heavily dependent on today. Several advantages are possible: zero day vulnerability and malicious code can be observed in the initial act of exfiltration resulting in faster response and increased efficiency of damage control countermeasures; decision making can be made with quantifiable risk and increased confidence when responding to new suspicious activity; the approach can be extended to a formal risk-based approach to attribution wherein investigative resources are allocated based on the probability that a data exfiltration event occurred. One potential and very important advantage of a formal risk-based approach to attribution is faster time-to-resolution of attribution of attack, which is of high value for cyber deterrence strategies.

Palacios and Kitten has alignment with cybersecurity complexity science analysis, and modeling, simulation and analysis of complex networked systems, while LDA statistical language analysis has alignment with informatics statistical TCP/IP anomalous behavior, cybersecurity mathematical and statistical analysis, and HPC analysis and correlation algorithms. Although the seven areas of research represent only a small segment of the potential science based research and analysis needed to address the national cyber dilemma, they represent game changing opportunity when coupled with the capability and mission of the NSCC.

The technological advancements in anomaly detection, advanced operating system virtualization and the NSCC could play a pivotal role HPC cybersecurity research.

A review of external open sources revealed a resonance with high level policy activities and identified similar research efforts. A December 2008 report [9] [Catlett] outlines the need to apply basic and applied research and engineering to the cybersecurity problem domain to move from a reactive to a proactive and predictive cyber defense posture. This report emphasizes mathematics: for predictive awareness for secure systems; Information: self protecting data and software; and platforms: trustworthy systems from untrusted components. We find there are common theme, purpose and vision presented in this report and the December 2008 "Scientific Research and Development Approach to Cyber Security" report.

Noted in the December 2008 report is the President's Information Technology Advisory Committee (PITAC) and the President's Council of Advisors on Science and Technology (PCAST)[10]. The PCAST shall serve as the advisory committee identified in subsections 101(b) and 103(b) of the High-Performance Computing Act of 1991 (Public Law 102-194), as amended

[9] A Scientific Research and Development Approach to Cyber Security, Submitted to the Department of Energy On Behalf of the Research and Development Community, December 2008. Comments to Charlie Catlett, Argonne National Laboratory

[10] http://www.whitehouse.gov/administration/eop/ostp/pcast

(15 U.S.C. 5511(b) and 5513(b)). In performing the functions of such advisory committee, the PCAST shall be known as the President's Innovation and Technology Advisory Committee[11].

PITAC cybersecurity research priorities include:

1. Authentication Technologies
2. Secure Fundamental Protocols
3. Secure Software Engineering and Software Assurance
4. Holistic System Security
5. Monitoring and Detection
6. Mitigation and Recovery Methodologies
7. Cyber Forensics: Catching Criminals and Deterring Criminal Activities
8. Modeling and Testbeds for New Technologies
9. Metrics, Benchmarks, and Best Practices
10. Non-Technology Issues That Can Compromise Cyber Security

We assert that the recommended areas of research and potential benefits presented herein are in full support of the PITAC cybersecurity research priorities.

[11] http://www.whitehouse.gov/the-press-office/executive-order-presidents-council-advisors-science-and-technology

### *3.3.1 Fundamental Relationships, Integration and Potential Benefits: Assessment Conclusions*

1. A holistic balanced cyber response capability is essential for the development of a comprehensive set of solutions.

2. An integral relationship of function and security as opposed to function vs. security is fundamental to a comprehensive national cyber defense capability.

3. The NSCC provides an established facility for continued cybersecurity HPC analysis and national cyber defense development.

4. Advanced automation (virtualization/Cloud Computing) provides an advantage of scale applicable to HPC platforms for advanced computing research and analysis.

5. Modeling and simulation of very large complex systems may reduce cost and time-to-deployment of wide-area national cyber defense technologies.

6. Statistical language analysis enables anomaly detection that is a departure from the signature and rules based dependence of extant cybersecurity protection methods.

7. Potential LDA anomaly detection advantages include zero day detection at initial act of exfiltration.

8. LDA anomaly detection can be extended to a formal risk-based approach with faster time-to-resolution and high value cyber deterrence benefits.

9. New insights are emerging with mathematical techniques associated with probabilistic latent semantic analysis.

10. The areas of research, the identified areas of impact and the actionable results are in support of the PITAC cybersecurity research priorities.

# 4. WIDE-AREA CYBERSECURITY DESIGN SPACE

## 4.1 Cybersecurity in an Ecosystem

*Goal: Develop characterization of cybersecurity in an ecosystem suitable to HPC research and development.*

The cyberterrain areas of concern pertaining to this phase of assessment are:

1. Threat & Vulnerability
2. Safeguards and Countermeasures
3. Risk Management
4. Prevention and Protection
5. Information Management
6. Detection and Warnings
7. Investigation and Response
8. Leadership and Authority
9. Resource Requirements
10. Workforce and Defenders
11. Coordination and Communication
12. Science and Engineering
13. Evaluation and Analysis
14. Actionable Results

The Internet is global and multicultural. Similarly, the cyberterrain intersects all cultures as a global entity. For the purpose of this report, please consider that horizontal cultures exhibit behavioral commonality due to shared environment, history, tradition and belief. Differing horizontal cultures can be greatly diverse, for example, eastern and western cultural differences. Vertical cultures also factor in the cyberterrain ecosystem. For example, consider the global cyber workforce as a vertical culture that spans a spectrum of skills and behaviors with impact to the cyberterrain: computer scientists; software engineers; hardware engineers; systems and process engineers; cybersecurity professionals; telecommunication engineers; and technically savvy enthusiasts comprise a vertical culture of common interest from richly diverse horizontal cultures. Cyberterrain sub-cultures exist in the world-wide audience of Internet users based on geopolitical, economic or other factors of affiliation. The resultant cyberterrain ecosystem is therefore culturally and technologically intertwined as technology is invented and exercised at the discretion of many human directives.

The power grid, national and international banking infrastructure, USG civil, judicial, and executive branches, national defense, as well as state, county and municipal emergency services are dependent and interdependent on network and information systems availability. Integration and shared risks are increasing due to critical dependence on information systems and the automation that they provide.

The scope and complexity of the cyberterrain includes cloud computing, and supervisory, control and data acquisition systems (SCADA). The function and functional interfaces of this

interconnected system of systems represents the level of challenge involved in modeling critical infrastructure and the ways in which they operate and interact.

Cybersecurity analysis applications in high end computing (HEC) or HPC are relatively new and therefore not well defined or understood on a broad scale. The modeling and simulation of wide-area interconnected systems entails coupled model components equivalent to that of a global ecosystem. Decomposition of the problem domain into defined subsystems will in large part drive the software codes needed for analysis. New requirements for computationally or I/O intensive cybersecurity applications will be based on the specific problems to be analyzed, the efficiency of the codes and algorithms available, and the system processor, memory and I/O performance necessary to scale parallelism for fast time-to-solution.

Characterization of cybersecurity HPC analysis in an ecosystem can be described as a compilation of characteristics from other areas of HPC analysis. Consider that cybersecurity complexity embodies the technical characteristics of signals intelligence analysis, the inherent interdependency characteristics of climate modeling, and the entity relationship characteristics of human/organizational systems studies[12] [NRC].

A quote from Getting Up To Speed: The Future of Supercomputing describes in part "Intelligence analysis begins with the output of IP and seeks to transform the blizzard of communications messages into a complete mosaic of knowledge so that adversaries' intentions are discerned and actionable intelligence provided to national leadership and others with a need to know." This serves as an apt description for cybersecurity analysis on the scale of the national information infrastructure.

Human and organizational systems studies are also relevant to the national cyber dilemma. This HPC analysis area studies macroeconomics and social dynamics, and hence the behavior of large human populations is simulated in terms of the overall effect of decisions by hundreds of millions of individuals. This is comparable to a world-wide cyber population.

Climate modeling is described as a composition of several major components of the climate system. These include an atmosphere model, an ocean model, a combined land-vegetation-river transport (hydrological) model, and a sea ice model. Consider that the national information infrastructure is similar in scope and complexity with human, cultural, organizational, legal and technical interdependent models.

From the ecosystem perspective, consider the need for modeling system behavior based on how information and technology are manipulated for human productive or malicious intent. Government, commercial, academic, nation state and citizen actors are part of potentially very intricate coupled model components. In addition, the participation of key stakeholders (government, academic, vendor, commercial and public communities), and decision makers which represent autonomous areas of authority and responsibility are also part of the human model in the cyber ecosystem. Hence, the study of cyber psychology and sociology of attacker/defender behavior, as well as massively multi-actor modeling and simulation will provide insight into phenomena such as cyber mob behavior.

[12] National Research Council 2005 publication, Getting Up To Speed: The Future of Supercomputing

We find that the concept of HPC analysis in near real time is largely dependent on geography in the cyberterrain. Threat data proximity and data transport time (latency) to an HPC analysis facility, computational time-to-solution, and response data transport time back to defenders and defense devices are all factors in the timely response to attack. Data integrity is also a mitigating factor, whereby the cleaner or more specific the dataset the faster the time to resolution of a problem.

When considering the cyberterrain as an ecosystem one can begin to understand the scope and complexity in terms of model variability. Also consider that the problem is increasing with the proliferation of technology world-wide. Distributed data collection and future petascale and exascale supercomputing analysis are anticipated requirements to adequately address a national cyber dilemma of increasing complexity.

The game board interpretation provides definition of cybersecurity in the context of a technical, organizational and human ecosystem. We find that this full spectrum or holistic approach is needed to address the broad scope of an environment on the scale of the national information infrastructure. Consider that the cyberterrain ecosystem consists of autonomous areas of authority interconnected via a network of networks with business dependencies and inter-dependencies conducted through a system of systems containing complexly varied and valuable types of information – in an aggressive threat environment.

Defense in the cyberterrain ecosystem is a daunting problem. A call to arms is on order to change the game board through science and technology, evaluation and analysis, and actionable results.

### *4.1.1 Cybersecurity in an Ecosystem: Assessment Conclusions*

1. The composition and complexity of wide-area cybersecurity on the scale of the national information infrastructure is commensurate to an ecosystem.

2. Culture and technology are intertwined as technology is exercised at the discretion of human directive.

3. The knowledge gained through HPC analysis and evaluation may prove vital to meet the needs for economic, civil, and national security assurance because of sweeping vulnerability and national information asset protection fragmentation across the national information infrastructure.

4. Cybersecurity systems architecture of the wide-area cyberterrain requires the participation of key stakeholders (government, R&D, vendor and commercial communities) and decision makers to resolve the shared risks introduced by interconnectivity via a common infrastructure.

5. The concept of HPC analysis in near real time is largely dependent on threat data proximity and data transport time (latency) to the HPC analysis facility because of the latency in data

transport and computational analysis involved with moving data from the source to analysis and back.

6. Distributed sensor networks and HPC cybersecurity analysis need to be considered together as one system of data collection, analysis and response to ensure sufficient throughput and performance end-to-end.

7. Data integrity is a mitigating factor that introduces the need for data filtering and aggregation to facilitate faster the time-to-resolution of a problem end-to-end.

8. Distributed data collection and future petascale and exascale supercomputing analysis are anticipated requirements to adequately address the increasing complexity of the cybersecurity dilemma and technology proliferation throughout the national information infrastructure.

9. A full spectrum or holistic approach is needed to address the broad scope of an environment on the scale of the national information infrastructure.

## 4.2 Wide-Area Conceptual Design Space

Goal: *Expand the dialog and understanding of the wide-area cyberterrain design space.*

The cyberterrain areas of concern pertaining to this phase of assessment are:

1. Threat & Vulnerability
2. Safeguards and Countermeasures
3. Risk Management
4. Prevention and Protection
5. Information Management
6. Detection and Warnings
7. Investigation and Response
8. Workforce and Defenders
9. Coordination and Communication
10. Science and Engineering
11. Evaluation and Analysis
12. Actionable Results

The wide-area design space assessment started with an assessment of common baseline technologies, platforms and providers in the global Internet as illustrated in figure 13. A simple premise is implied: *friendly and adversarial investments in widely distributed commercial off the shelf (COTS) products establish globally well known use and knowledge of function, vulnerability and exposure*.

The wide-area design space defense posture is largely dependent on network perimeter security with rules based border router, web proxy, and firewall protection mechanisms. System security

is largely dependent on previously observed signature based antivirus and intrusion detection systems.

Enterprise information system security is largely dependent on three key automation technologies:

- Identity and Access Management (I&AM)
- Network Configuration Management (i.e. Policy Based Network Management (PBNM))
- Service Oriented Architecture (SOA).

The Internet is a constantly changing set of services, applications, systems and infrastructure components with consumer facing, command and control, and operational support interfaces for global processing, transmission and storage of information. Global interconnectivity is built on routed and routing protocols, a variety of switching technologies, and a myriad of versions of operating systems on varied platforms. Internet protocols present another area of complex differentiation. Consider for example that the Internet Protocol is comprised of IP version 4 (IPv4) and IP version 6 (IPv6), two vastly different structures of communication. In addition, variations in wide-area network (WAN) infrastructure must be considered, such as passive optical networks (PON), and asynchronous transfer mode (ATM), along with the specific vulnerabilities inherent to each technology.

Feature, function, integration, customization and performance are all differentiating factors. Infrastructure segments and each enterprise are unique and complex sub-systems comprised within the cyberterrain ecosystem.

It is equally important that secure software development and validation accompany advances in trusted hardware. An increased investment in terms of time, resources and funding is needed to enable these advancements. Secure software development and trusted hardware are codependent requirements for secure information systems in the wide-area design space and are essential factors to be considered in the cyberterrain ecosystem.

A notional systems-of-systems architecture for wide area cybersecurity data collection and analysis may include the following system elements:

1. High Speed Sensor Networks
2. Correlation Algorithms
3. Distributed Data Transport
4. HPC Large-Scale Computation
5. Analysis Algorithms
6. HPC I/O Communications
7. High Performance Database and Storage

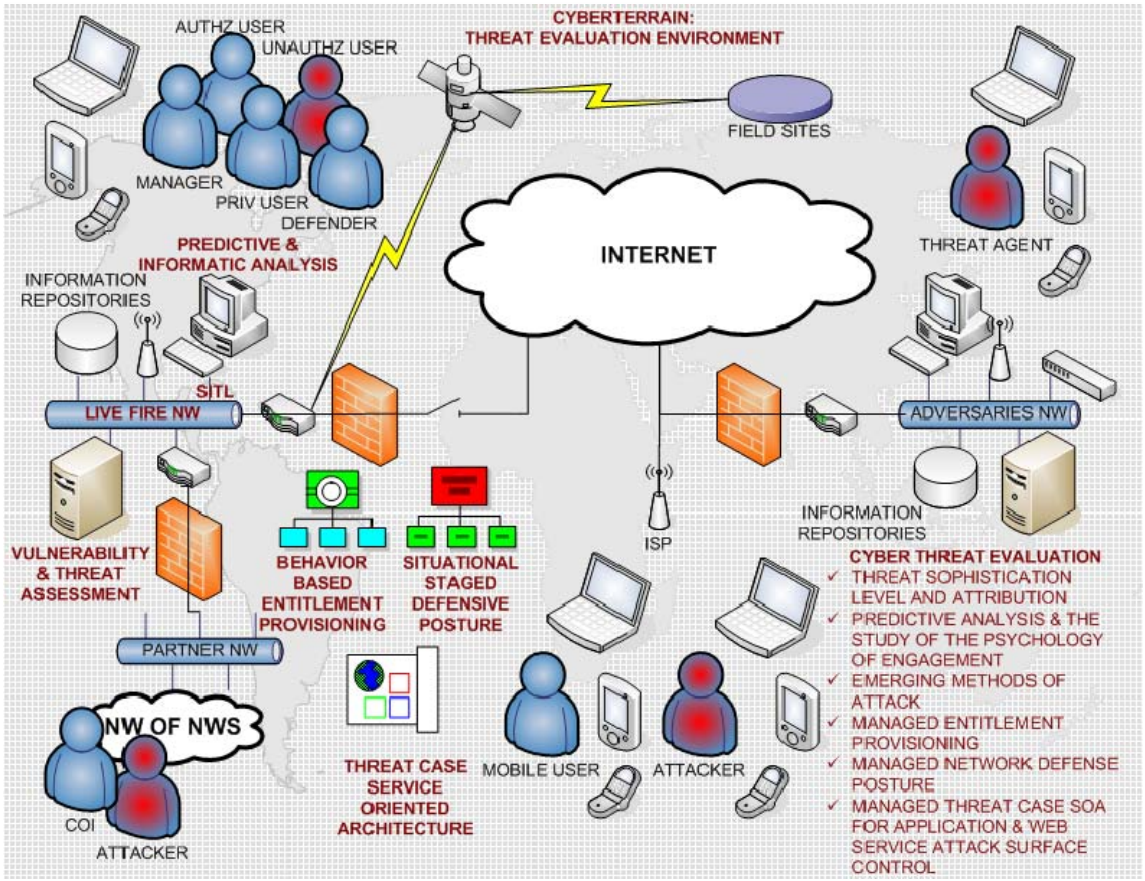


**Figure 13: Conceptual Cyberterrain Wide-Area Threat Evaluation Environment**

In this conceptual wide-area threat evaluation environment the infrastructure and technology investments of domestic and foreign entities are similar and familiar to a global workforce.

Note that the three key automation technologies of I&AM, PBNM and SOA are extended respectively to:

- Behavior Based Entitlement Provisioning
- Situational Staged Defense Posture
- Threat Case SOA.

The threat evaluation environment would permit the study of attack and defense behavior for development of predictive and preventative technologies. Wide-area threat evaluation environment data can be used for Informatics analysis, emulation of complex networked systems, and the development of embedded attributes for provenance and discovery. The evaluation capability would allow cybersecurity interactive attack and defender exercises, such as capture the flag, which could be carried out on the scale of national interests.

The utility of I&AM is expanded to a provisioning behavior-based entitlement capability for graded control of varied levels of user entitlements and permissions. Both cyber defender and threat actor identities can be managed in this way. The utility of automated device configuration

management is expanded to a provisioning capability for graded control of network access paths for users, devices and applications. Lastly, the utility of SOA and virtualization are expanded to a provisioning capability for graded control of external facing web services.

These technologies provide a means of managing three of the primary attack surfaces available to an adversary and can be used to gage the level of sophistication necessary to breach increasing levels of protection.

Threat environment evaluation can be envisioned as a honey-pot where aggregate computer and network defenses are approximated and tested against various levels of sophisticated threat. Testing would be interactive with threat-agent and defender behaviors played out over time in changing situational conditions much like massively multi-player online gaming. Live-interactive networks could enable a test environment with physical network devices and paths for cyber-security maneuvers. Combined, these capabilities could provide a foundation for wide-area coordinated attack and recovery evaluation, validation of new national cyber-defense strategies, and facilitate cross-organizational training for cyber-defense personnel.

The integration of modeling and simulation with live interactive networks offers an arena for the evaluation of emerging cyber-threats and the validation of national cyber-defense mission capability to recover from attack. Possible areas of opportunity for evaluation and validation are discussed below.

**Evaluation of Changing Attack Methods and Shared Risk Exposure**

Critical dependence on information technologies worldwide places cyber-dominance at the forefront of a new battlefield. Cross-organizational evaluation of shared risk exposure of interconnected networks is needed to confront the global cyber-threat. Evaluation of various defense postures against multi-stage and polymorphic attacks is needed to validate and ensure appropriate wide-area protection, response, and recovery to sophisticated attack. An example test concept for countering changing attack methods is a compartmented or modular cyber-defense architecture to provide resilience and increased survivability to attack.

**Evaluation and Validation of National Cyber-Defense Preparedness**

The validation of coordinated cyber-defense capabilities across multiple organizations is needed as risk to the national information infrastructure increases. Evaluation of attack and recovery through simulated attack scenarios could provide a baseline for national cyber-defense preparedness. For example, simulated attack methods can be used across a wide-area test environment to gage preparedness without impacting critical information resources. Weaknesses, such as gaps in continuity of operations plans (COOP) could be identified and resolved through coordinated evaluation.

**Evaluation and Validation of Wide-Area Cyber-Defense Methodologies**
Evaluation and validation of developing wide-area cyber-defense methodologies is needed to assure a strengthened national cyber-defense protection posture. For example, assessment of the efficiency of new intrusion and anomaly detection methods across the wide-area infrastructure would reduce costly discovery of inefficiencies after deployment. Additionally, virtual exercises of coordinated response to attack to test timely notification and reporting of attack across multiple organizations would not disrupt operations or require the resources needed for live preparedness exercises on a large scale. New defense concepts will require validation to assure successful global deployment and support.

**Evaluation and Validation of Wide-Area Cyber-Operation Methodologies**
As new wide-area cyber-defense methodologies emerge so will new wide-area methods of operation. For example, better definition of collaborative COI and local enforcement of need-to-know protection mechanisms are needed as connectivity increases and access to sensitive information is expanded to users on external networks. New enterprise operational concepts will require validation to assure successful global deployment.

Simulated attack and recovery would greatly benefit from reusable models that permit real-world threat scenarios to be sequenced or layered to emulate complex multi-staged attacks. Also system-in-the-loop (SITL) like interfaces that permit communication with live network agents (automated or human threat-actors and defenders) will be fundamental to interactive use. Another challenge is the development of real-time detection and response to changing threat with models that are well-defined for specific attacks against specific vulnerabilities. Furthermore, the identity and behavioral characteristics of threat-agents and defenders will need to be modeled such that threat scenarios are temporal and interactive. Ideally, an identity and behavior enabled model would comprise a threat-actors' level of sophistication and means of attack against the aggregate defenses of interconnected networks.

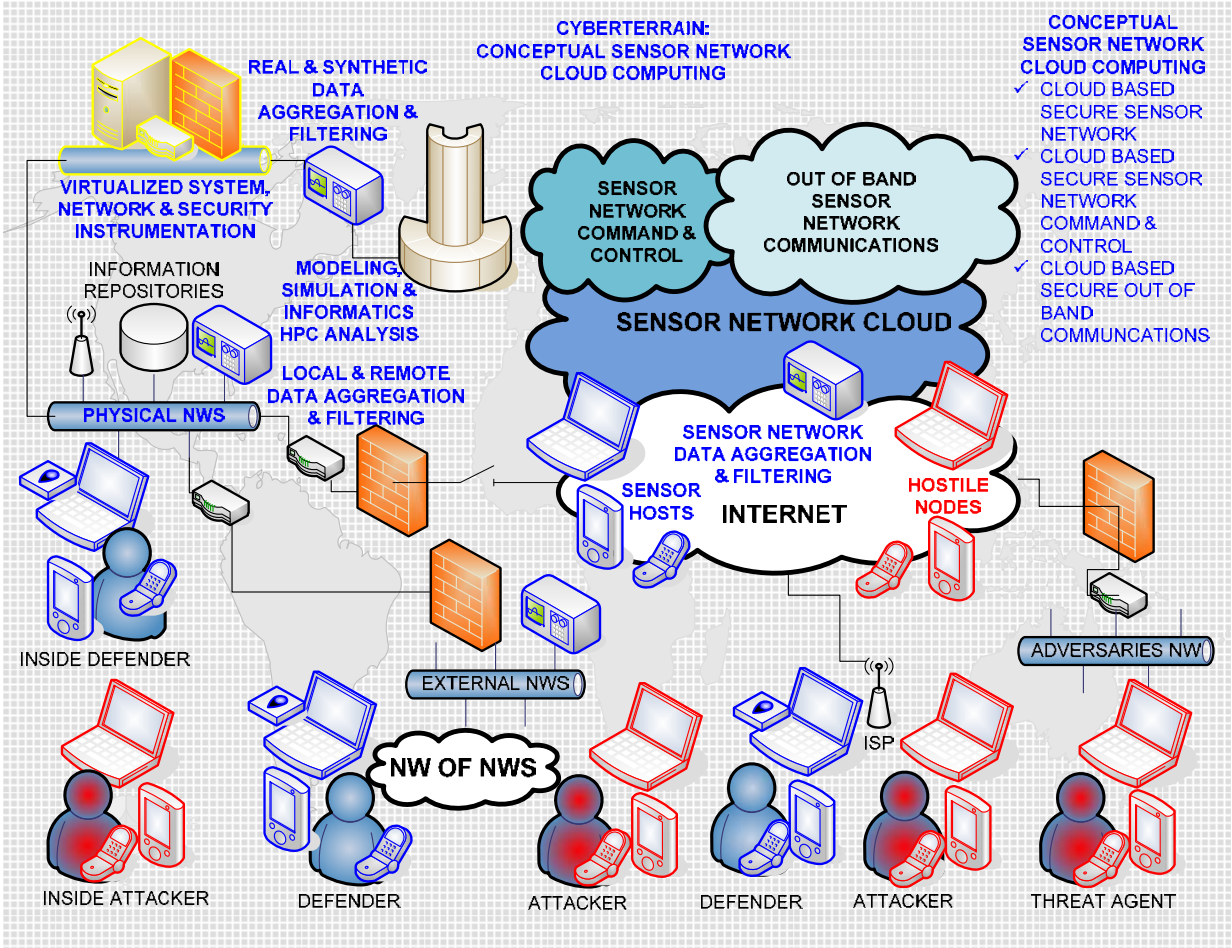


**Figure 14: Conceptual Cyberterrain High Speed Distributed Sensor Environment**

A distributed high-speed sensor network would augment the security and utility of the cyberterrain with a means of early warning indicators. Wide-area data collection requires sensors for live data collection and correlation algorithms to manage large volumes of data. Processing of correlated events or more detailed datasets could be filtered and aggregated for off-line or HPC accelerated processing. It should be noted that real-time processing is largely dependent on dataset locality to analysis and transport time to/from the data source.

Sensor network architecture includes command and control and out-of-band (OOB) data paths to fulfill the national cybersecurity mission. This system of systems will comprise distributed sensors and sensor networks, transport filters, aggregation and transport, as well as the I/O, processing, and storage capabilities required for a sustainable system that permits network defenders real-time interactive operations.

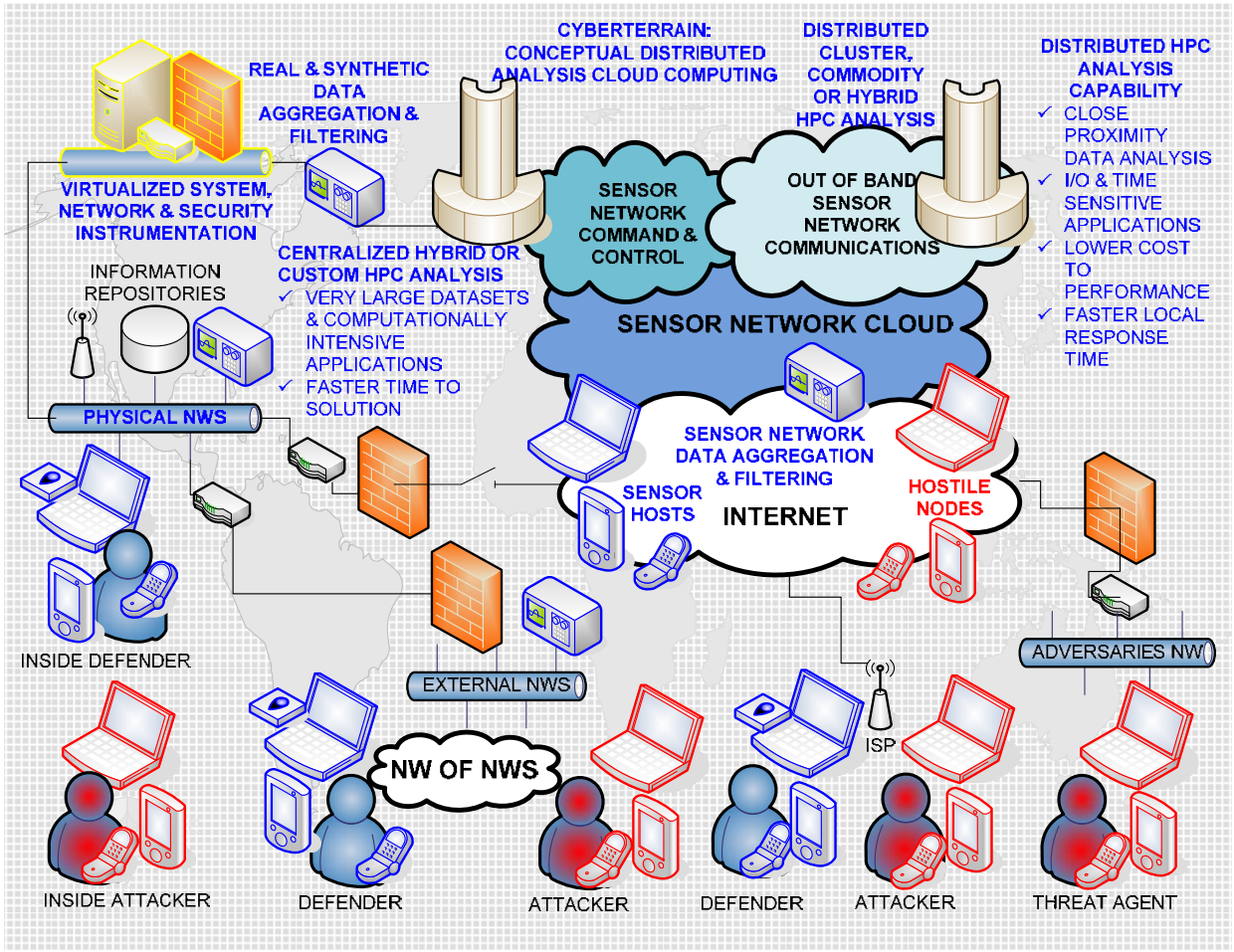


**Figure 15: Conceptual Cyberterrain Distributed HPC Analysis Environment**

Illustrated in figure 15 is a conceptual distributed high-speed sensor network and analysis cloud. Wide-area data collection requires high-speed sensor network data collection and correlation algorithms, while analysis is dependent on algorithms, code, high performance storage and file system, and a database capability to support simultaneous, multiple, fast read and writes on extremely large data sets.

HPC system I/O has to be able to handle large data movements without congestion to meet the need for real-time interactive operations. Note that distributed cost-to-performance capacity cluster, commodity or hybrid HPC systems are located near the edge or in close proximity to the data source for near real-time fast I/O HPC accelerated processing. Conversely, faster time-to-solution hybrid or custom capability HPC systems for off-line or HPC accelerated processing are centralized.

Cybersecurity communications must be held to high level of confidentiality and integrity standards that enable trusted operation, including wide-area data collection, effective wide-area protection posture, and assured critical access and operations.

### *4.2.1 Wide-Area Conceptual Design Space: Assessment Conclusions*

1. The defense posture perimeter is largely dependent on rule based device security, such as border router, web proxy, and firewall protection mechanisms.

2. System security is largely dependent on signature based antivirus and intrusion detection systems.

3. An increased investment in terms of time, resources and funding in secure software development and validation, and trusted hardware as codependent requirements is needed for national cyber defense advancements.

4. Enterprise information system security is dependent on three key automation technologies: I&AM; PBNM; and SOA.

5. Domestic and foreign infrastructure and technology investments are similar and familiar to a global workforce.

6. Conceptually, I&AM, PBNM and SOA can be extended to Behavior Based Entitlement Provisioning, Situational Staged Defense Posture, and Threat Case or Rapid Response Virtualized SOA a means of managing primary attack surfaces available to an adversary.

7. The integration of modeling and simulation with live interactive networks offers an arena for the evaluation of emerging cyber-threats and the validation of national cyber-defense mission capability to recover from attack.

8. Conceptually, distributed high-speed sensor networks and cluster, commodity or hybrid HPC systems, which are co-located or in close proximity to the data source, could perform near real-time fast I/O HPC accelerated processing.

9. Conceptually, centralized hybrid or custom architecture HPC systems would perform fast time-to-solution off-line or HPC accelerated processing for large dataset or computationally intensive processing.

10. Cybersecurity communications must be held to high confidentiality and integrity standards that enable trusted operation.

## 4.3 Related Impacts in the National Threat and Defense Posture

Goal: *Investigate the national cyber defense posture for related impacts to wide-area national cyber defense.*

The cyberterrain areas of concern pertaining to this phase of assessment are:

1. Threat & Vulnerability
2. Safeguards and Countermeasures
3. Risk Management
4. Prevention and Protection
5. Information Management
6. Detection and Warnings
7. Investigation and Response
8. Leadership and Authority
9. Resource Requirements
10. Workforce and Defenders
11. Coordination and Communication
12. Science and Engineering
13. Evaluation and Analysis
14. Actionable Results

Fundamental to the advancement of a national cyber defense posture are executive leadership, organizational commitment and funds availability. Without these fundamental tenets progress is severely inhibited.

Comprehensive National Cybersecurity Initiative

The activities under way to implement the recommendations of the Cyberspace Policy Review build on the Comprehensive National Cybersecurity Initiative (CNCI)[13]. President Obama determined that the CNCI and its associated activities should evolve to become key elements of a broader, updated national U.S. cybersecurity strategy. To improve public understanding of Federal efforts, the Cybersecurity Coordinator has directed the release of a summary description of the CNCI[14].

The CNCI consists of a number of mutually reinforcing initiatives with the following major goals designed to help secure the United States in cyberspace:

1. To establish a front line of defense against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and ultimately

[13] The Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23) in January 2008.
[14] http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions.

2. To defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.

3. To strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

Published CNCI Initiative details include the following 12 initiatives. For complete information please refer to references noted.

1. Initiative #1. Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections. The Trusted Internet Connections (TIC) initiative covers the consolidation of the Federal Government's external access points.

2. Initiative #2. Deploy an intrusion detection system of sensors across the Federal enterprise. Intrusion Detection Systems using passive sensors form a vital part of U.S. Government network defenses by identifying when unauthorized users attempt to gain access to those networks.

3. Initiative #3. Pursue deployment of intrusion prevention systems across the Federal enterprise. This Initiative represents the next evolution of protection for civilian Departments and Agencies of the Federal Executive Branch.

4. Initiative #4: Coordinate and redirect research and development (R&D) efforts. No single individual or organization is aware of all of the cyber-related R&D activities being funded by the Government. This initiative is developing strategies and structures for coordinating all cyber R&D sponsored or conducted by the U.S. government, both classified and unclassified, and to redirect that R&D where needed.

5. Initiative #5. Connect current cyber ops centers to enhance situational awareness. There is a pressing need to ensure that government information security offices and strategic operations centers share data regarding malicious activities against federal systems, consistent with privacy protections for personally identifiable and other protected information and as legally appropriate, in order to have a better understanding of the entire threat to government systems and to take maximum advantage of each organization's unique capabilities to produce the best overall national cyber defense possible.

6. Initiative #6. Develop and implement a government-wide cyber counterintelligence (CI) plan. A government-wide cyber counterintelligence plan is necessary to coordinate activities across all Federal Agencies.

7. Initiative #7. Increase the security of our classified networks. We need to exercise due diligence in ensuring the integrity of these networks and the data they contain.

8. Initiative #8. Expand cyber education. It is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However there is not an adequately established Federal cybersecurity career field. We must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees.

9. Initiative #9. Define and develop enduring "leap-ahead" technology, strategies, and programs. One goal of the CNCI is to develop technologies that provide increases in cybersecurity by orders of magnitude above current systems and which can be deployed within 5 to 10 years. This initiative seeks to develop strategies and programs to enhance the component of the government R&D portfolio that pursues high-risk/high-payoff solutions to critical cybersecurity problems.

10. Initiative #10. Define and develop enduring deterrence strategies and programs. This Initiative is aimed at building an approach to cyber defense strategy that deters interference and attack in cyberspace by improving warning capabilities, articulating roles for private sector and international partners, and developing appropriate responses for both state and non-state actors.

11. Initiative #11. Develop a multi-pronged approach for global supply chain risk management. This initiative will enhance Federal Government skills, policies, and processes to provide departments and agencies with a robust toolset to better manage and mitigate supply chain risk at levels commensurate with the criticality of, and risks to, their systems and networks.

12. Initiative #12. Define the Federal role for extending cybersecurity into critical infrastructure domains. The U.S. Government depends on a variety of privately owned and operated critical infrastructures to carry out the public's business. In turn, these critical infrastructures rely on the efficient operation of information systems and networks that are vulnerable to malicious cyber threats. This Initiative builds on the existing and ongoing partnership between the Federal Government and the public and private sector owners and operators of Critical Infrastructure and Key Resources (CIKR). It addresses security and information assurance efforts across the cyber infrastructure to increase resiliency and operational capabilities throughout the CIKR sectors. It includes a focus on public-private sharing of information regarding cyber threats and incidents in both government and CIKR.

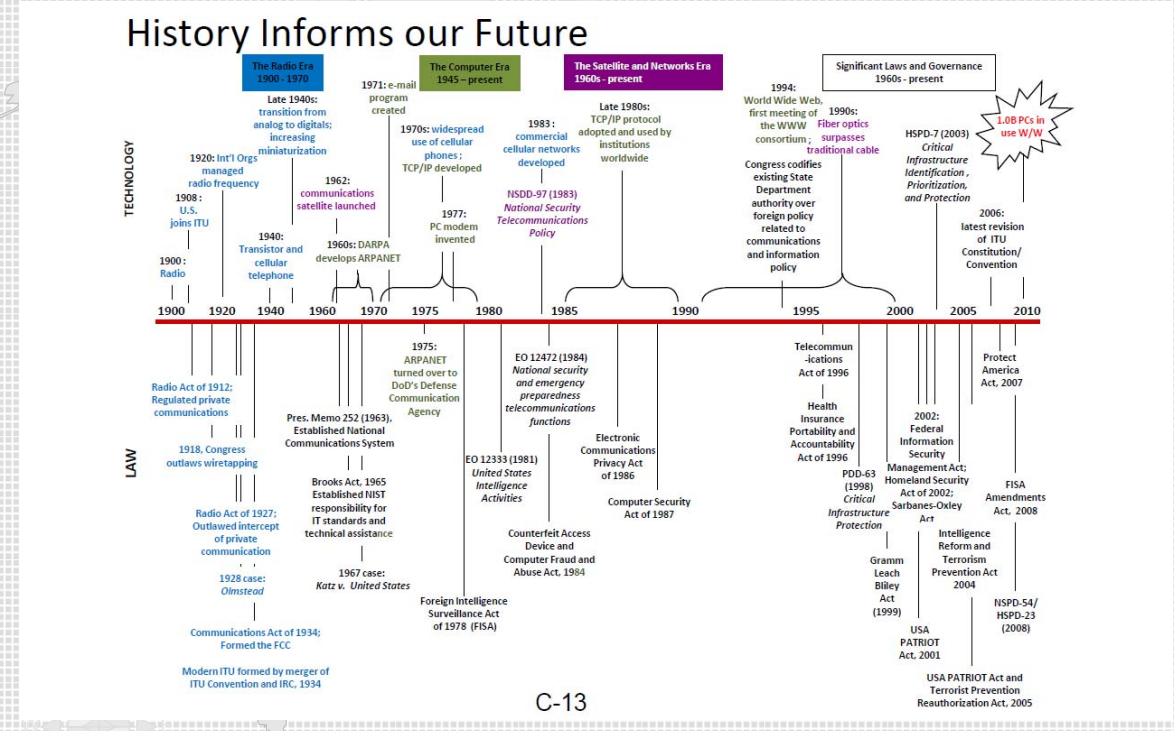


**Figure 16: History Informs Our Future**

Figure 16 illustrates a history of technology and law from the 2009 Cyberspace Policy Review[15]. More recently the Cybersecurity Act of 2010[16] includes an increase in support for national cyber defense development that includes: Title I - Workforce Development; Title II - Plans and Authority; Title III – Cybersecurity Knowledge Development; and Title IV – Public-Private Collaboration. Provided below are a few selected quotes from the Cybersecurity Act of 2010.

"With more than 85 percent of the Nation's critical infrastructure owned and operated by the private sector, it is vital that the public and private sectors cooperate to protect this strategic national asset."

"As a fundamental principle, cyberspace is a vital asset for the nation and the United States should protect it using all instruments of national power, in order to ensure national security, public safety, economic prosperity, and the delivery of critical services to the American public."

[15] History Informs Our Future: Cyberspace Policy Review, April 17, 2009
[16] http://commerce.senate.gov/public/index.cfm?p=Legislation&ContentRecord_id=f2256d47-85a9-4c64-b9e0-40ab01564735

“According to the 2010 Annual Threat Assessment, that ‘‘sensitive information is stolen daily from both government and private sector networks’’ and that ‘‘we cannot protect cyberspace without a coordinated and collaborative effort that incorporates both the US private sector and our international partners.’’”

Coordination is a hard problem to solve because it requires a trusted operational foundation where authority, roles, and responsibilities are understood and cyber rules of engagement are practiced. Accountability is also a necessity for the robustness for wide-area cybersecurity, for example enforceable non-repudiation to hold individuals accountable to inappropriate action and misuse of information.

Consideration for a national cyber defense warrants a larger design space that spans the fourteen Cybersecurity domains of concern within the cyberterrain. There is a long history of technological innovation, civil liberty and legal entanglement. Although very complex with the competing principles of civil liberty and national security, this history sets precedent for the development of national cyber defense in step with evolving threats to national security.

The global Internet cyberterrain is not as encumbered by well-formed law. The disparate ideologies and legal frameworks across the globe are likewise relevant to the cyberterrain. Internationally conducted identity theft and black market sales are difficult at best to investigate and prosecute and perpetrators often operate with impunity.

### *4.3.1 Related Impacts within the National Threat and Defense Posture: Assessment Conclusions*

Without strong executive leadership, organizational commitment and funds availability progress for the advancement of a national cyber defense posture is severely inhibited.

The Comprehensive National Cybersecurity Initiative provides relevance and value for cyberterrain evaluation and the development of a national cyber defense posture.

The history of technological innovation, civil liberty and legal entanglement sets precedent for the development of a national cyber defense capability.

# 5. SOLUTION SPACE CONCEPTS OF OPERATIONS AND ROADMAPS

## 5.1 Solution Space Concepts of Operation

Goal: *Develop conceptual wide-area cyberterrain solution scenarios.*

The solution space will be expanded through science and technology research and broad coordination. In support of this notion we have provided several concepts of operation and possible positive outcomes for national cyber defense.

The integration of simulated threat and live interactive networks offers a proactive means to evaluate the characteristics of interconnected networks and to validate national cyber-defense mission capabilities. Current network modeling and simulation technology permits interoperation with live networks but lacks a sophisticated threat simulation capability with live interactive networks. The caveat is that many difficult technical and organizational challenges need to be resolved before such a capability is realized.

### *5.1.1 Value Based Information Protection Concept of Operations*

The cyberterrain areas of concern pertaining to this concept of operation are:

1. Prevention and Protection
2. Information Management

Value based information protection addresses the two aspects of information asset access: *the user or subject; and the information asset or object*. Value based information protection provides more granular information asset access control based on well defined COI and discoverability labels for information asset attributes. Value based information access controls can be applied to intranet and internet COI as appropriate for a taxonomy of information assets.

1. Embedded Discoverability Attributes (Sensitivity Value)
    - Fully Discoverable
    - Metadata Discoverable
    - Restricted Metadata Discoverable
    - Discovery Exempt

2. Embedded Provenance Attributes (Trusted Information and Source)
    - Non-Repudiation
    - Integrity

3. Well Defined Communities of Interest (Positive Access Control)
    - Internal Authorized Users & Groups
    - Privileged Role Based Accounts
    - Collaborative Partner Trust Relationships
    - External Unclassified & Public Information

### *5.1.2 Cyber Personification Schema Concept of Operations*

A Cyber Personification Concept of Operation is an example of a new wide-area cyber-operation method.

The cyberterrain areas of concern pertaining to this concept of operation are:

1. Threat & Vulnerability
2. Safeguards and Countermeasures
3. Information Management
4. Detection and Warnings
5. Investigation and Response
6. Coordination and Communication

The risks of intrusion and compromise are increasing as dependence on automated information systems grows amid evolving technologies, changing policy guidance, expanded access requirements, global connectivity, and an active Cyber threat. Cyber personification is designed to address each of these risk factors for a more secure national information infrastructure by: strengthening access-control for well-formed collaborative COI; accounting for the adoption of new technologies; and increasing the security posture for integrated organization to organization information environments.

Cyber personification comprises a standardized personification schema with a composite index of persona identifiers, information environment descriptors, and electronic device capability descriptors that provide consistent and authoritative metrics for cybersecurity decision making processes. A standardized personification solution will provide a foundation for well-managed cybersecurity that is cost effective and scalable to global deployments while delivering a structure for the development of secure collaborative information services and new protocol designs.

Cyber personification will change the game board by providing well-formed collaborative or external COI requiring access to intranet information environments. This will set the stage for enforceable rules of conduct for authorized players while strengthening the protection posture against malicious identities and entities whose unauthorized access to information assets pose significant threat. Electronic device capabilities are also articulated to address an integral shift in information technology that must be included in the game space.

Cyber personification would serve to address the dynamics of wide-area information service delivery and rapid deployment communication environments. Specific COI security-domain relevance could be determined with standardized identity, environment, and device attributes that represent broad need-to-share directives while ensuring the need-to-know integrity of local information assets.

Access entitlements would be captured in a multidimensional description of the subject (user or entity acting on behalf of the user and methods of access) and the object (information assets within the information environment). The dimensions comprise global, local, and anonymous

entitlement profiles for membership of each COI that may be further defined by specific rights for each intranet information environment. Similarly, discoverability labels for information assets (value based information protection) would pair with COI entitlements to ensure protection while permitting authorized access (see *Principles of Operation* below).

The personification vision is based in the identity and access management (I&AM); service oriented architecture (SOA); and security technologies that are in use today. Organization to organization integration is difficult and cohesive solutions are evasive. Collaboration systems are often crippled by trust issues, proprietary technologies, economic constraints, or business, policy and technology investment differences between organizations that need to share information. To fill the gap created by the proliferation of technology, expanded access requirements and global connectivity, and to effectively confront the active Cyber threat, we must think globally.

*Principles of Operation* - three principles of operation are assumed:

*Containment Principle* - local cybersecurity policies take precedence over foreign entitlement assertions.

*Discoverability Principle* - information assets are implicitly globally discoverable, unless explicitly identified as fully metadata discoverable, limited metadata discoverable, or exempt from discovery.

*Portability Principle* – a standardized format with associative data dictionary and glossary are used for the personification schema, index, identifiers, and descriptors.

The objective is to capture the expanding scope and dynamics of the game board in a standard schema and quantifiable measure such that all authorized players, their capabilities, access permissions and entitlements to information assets are known and manageable to mitigate risk (Table 2: Risk Factors and Personification Risk Mitigation).

**Table 3. Factors and Personification Risk Mitigation**

| Risk Factors | Personification Risk Mitigation |
|---|---|
| Intrusion via loosely defined access-control | Personification schema & composite index |
| Changes in Need-To-Share and Need-To-Know policy | Global, local and anonymous security-domain relevance via COI identifiers |
| Global connectivity and increased mobility of users | Composite location, COI, and associated authorization identifiers |
| Service oriented architectures | Service type descriptor (web, network quality of service, virtualized, simulated/interactive) |
| Increased discoverability of centralized information assets | Information asset discoverability descriptors (globally discoverable, fully metadata discoverable, limited metadata discoverable, or exempt from discovery) to be matched with specific global, local, and anonymous COI entitlements |
| Convergence of multimedia data types (voice, video and data) | Complex-data descriptors to indicate composite data types and/or associated attachment data types |
| Electronic recording, transmitting and wireless enabled devices | Fixed or mobile device capability descriptors, may include mobility zones (location) and associated authorization/restriction attributes such as time of day or user/group. |

### *5.1.3 Distributed Detection, Notification and Response Concept of Operations*

The cyberterrain areas of concern pertaining to this concept of operation are:

1. Threat & Vulnerability
2. Safeguards and Countermeasures
3. Risk Management
4. Prevention and Protection
5. Detection and Warnings
6. Investigation and Response
7. Workforce and Defenders
8. Coordination and Communication

A distributed detection, notification and response framework will change the game board by providing a means of uniform wide-area electronic notification of suspicious or confirmed malicious events to centralized or regional analysis and response centers. This will set the stage for distributed intrusion and anomaly detection or prevention systems to report malicious activity for coordinated wide-area threat analysis and defensive response to cyber attack.

The distributed detection, notification and response concept is based on a framework of event correlation with common terms and definitions for the characterization of malicious activity across a wide-area of peer networks. Detection and prevention systems would notify centralized or regional Cyber intrusion analysis and response centers of malicious events. Notice and response traffic could be routed through peer-network aggregate collection points to support global scalability. Cyber intrusion analysis and response centers could further disseminate threat response information to the wide-area as necessary.

A field of 4 bits could represent sixteen levels of severity and scope of attack. Packet payload could be encrypted for confidentiality, with notice and response traffic sent as either connectionless for expedited delivery or connection-oriented for assured delivery. Communications could be transmitted via secure tunnel or IPSec for transmission over the Internet or multi-protocol layer switching (MPLS) infrastructure. Additionally, machine or identity Public Key Infrastructure (PKI) certificates could provide non-repudiation of authorized senders and recipients with digital signatures used for assuring the integrity of the message contents. For highly secure environments, notice and response traffic could be sent via point-to-point out-of-band channels.

Notice-of-intrusion packet payload could include behavioral and attack characterization data, while threat related response packets could include malicious code signatures and wide-area remedial actions based on analysis of the threat or attack. Such rapid response data could aid in the real-time analysis of attack for assessing attribution and the level of sophistication involved in Cyber attacks (Table 3: Cyber Threat Levels and Severity Indicators).

Intrusion event-correlation would conceivably deliver early warning notices of an attack from distributed or locally managed security systems across several sectors, for example, intergovernmental, financial, or SCADA infrastructure. Local incident response teams would be responsible for collecting forensics and evidentiary information such as source and destination IP addresses, server or email names, and methods of intrusion and compromise involved in the attack.

The vision is to capture the expanding scope and dynamics of attacks in quantifiable measure such that all parties responsible for reporting, responding to and recovering from attacks are aware and involved in the rapid response to wide-area or large-scale cyber intrusion and attack. The goal of the distributed detection, notification and response framework is coordinated and timely damage control, analysis, investigation, and recovery from attack involving multiple networks and response teams.

A distributed detection, notification and response solution will provide a foundation for coordinated cybersecurity incident analysis and rapid response that is cost effective and scalable to global deployments while delivering a structure for the development of assured inter-connectivity and new protocol designs.

*Principles of Operation* - three principles of operation are assumed:

*Notice of Intrusion Principle* - intrusion notification data will be characterized using common terms and definitions to keep traffic nominal but high value.

*Local Accountability Principle* – local response teams will be accountable to assess evidentiary information in support of coordinated analysis, investigation, and recovery from intrusion or attack.

*Portability Principle* – a standardized format and glossary are used for threat levels and severity.

**Table 4. Cyber Threat Levels and Severity Indicators**

| Cyber Threat Levels | Severity Indicators (binary and hex) | |
|---|---|---|
| Normal (all clear) | 0000 | 0 |
| Suspicious anomalous activity | 0001 | 1 |
| Suspicious low level malicious activity | 0010 | 2 |
| Suspected coordinated malicious activity | 0011 | 3 |
| Suspected sophisticated malicious activity | 0100 | 4 |
| Confirmed low level malicious activity | 0101 | 5 |
| Confirmed coordinated malicious activity | 0110 | 6 |
| Confirmed sophisticated malicious activity | 0111 | 7 |
| Suspected Cyber attack | 1000 | 8 |
| Suspected multi-point Cyber attack | 1001 | 9 |
| Suspected automated Cyber attack | 1010 | A |
| Suspected sophisticated Cyber attack | 1011 | B |
| Confirmed Cyber attack | 1100 | C |
| Confirmed multi-point Cyber attack | 1101 | D |
| Confirmed automated Cyber attack | 1110 | E |
| Confirmed sophisticated Cyber attack | 1111 | F |

### *5.1.4 Cyber Adaptive Response Architectures Concept of Operations*

The fundamental Cyber Adaptive Response Architecture (CARA) concept is staged defensive readiness to changing threat conditions. Well-managed secure access, infrastructure configuration, and information service delivery provide the foundation on which CARA is based.

The cyberterrain areas of concern pertaining to this concept of operation are:

1. Threat & Vulnerability
2. Safeguards and Countermeasures
3. Risk Management
4. Prevention and Protection
5. Detection and Warnings
6. Investigation and Response
7. Workforce and Defenders
8. Coordination and Communication

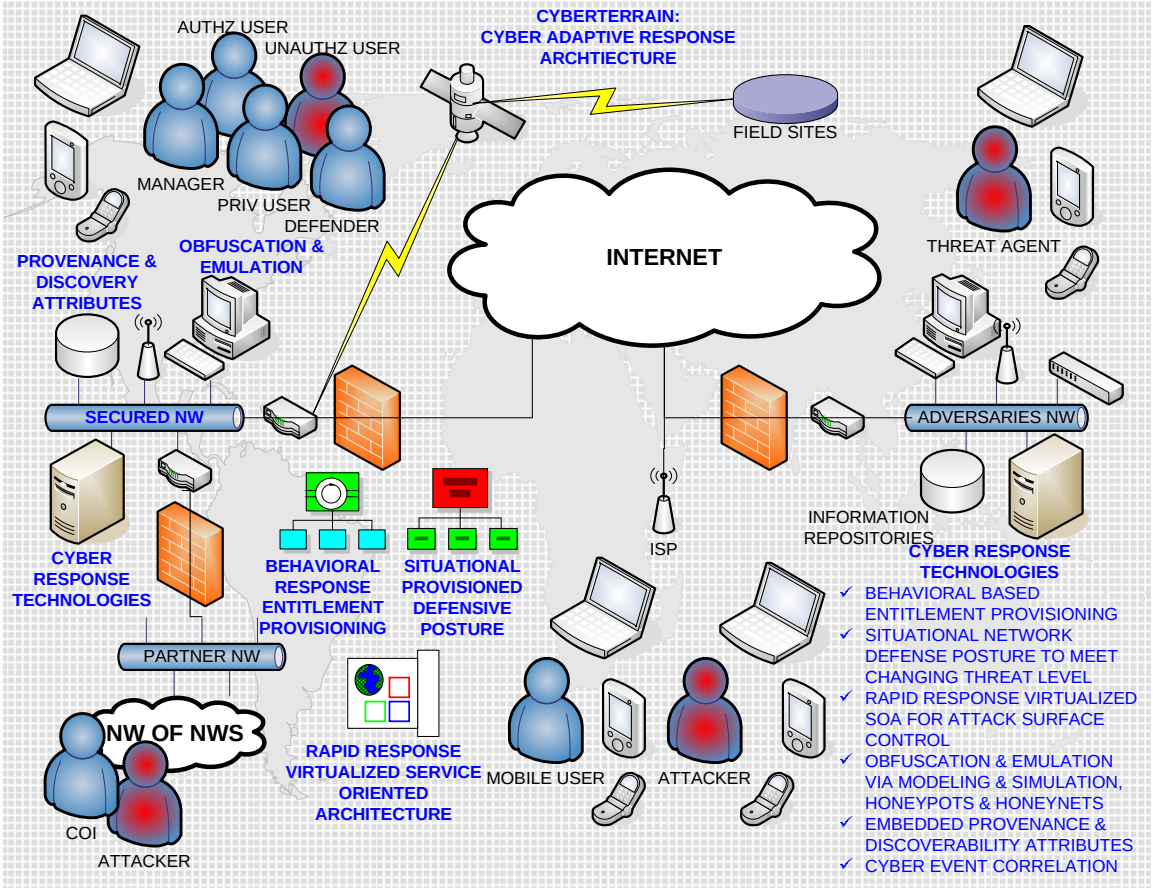


**Figure 17: Conceptual Cyberterrain Cyber Adaptive Response Architecture**

The knowledge gained from concerted threat evaluation could underpin a Cyber Adaptive Response Architecture based on the development of three key automated defense technologies:

- Behavior-Based Entitlement Provisioning
- Situational Provisioned Defensive Posture
- Rapid Response Virtualized SOA

*Behavior-based entitlement provisioning* would provide levels of entitlement, whereby the most permissive set of entitlements would accommodate normal operations. *Situational provisioned defensive* posture would be similarly automated through PBNM for levels of network functionality. Lastly, *rapid response virtualized SOA* would manage the attack surface to increasingly more secure external service posture as threat levels increase.

CARA would provide an enhanced assurance boundary with well defined protection ready to be rolled out in response to escalated threat conditions. Safeguards and countermeasures for technology investments that could be strengthened, for example response postures could be developed expertly for Microsoft Active Directory and for Oracle/Sun or Novell Directory Service deployments, each with the configuration nuance to platform specific configuration. When an immediate threat requires response, each technology investment could be leveraged in independent but coordinated fashion.

CARA comprises predefined sets of permissions, configuration profiles, and information service definitions that can be deployed for increased threat protection in rapid response to attack that can escalate as threat levels escalate.

The precedence for multiple postures to counter increasing levels of threat is provided by the threat definition matrix. A strategy following this paradigm would provide consistency and structure. Defense against automated staged attacks requires well-managed and robust automated protection-mechanisms for timely defensive response and damage control. The vision is to engineer well managed and adaptive first and fallback defenses to counter escalating threat levels in the age of information warfare and automated exploitation.

### *5.1.5 Scalable Cyber Threat Definition Concept of Operations*

The cyberterrain areas of concern pertaining to this concept of operation are:

1. Threat & Vulnerability
2. Risk Management
3. Coordination and Communication

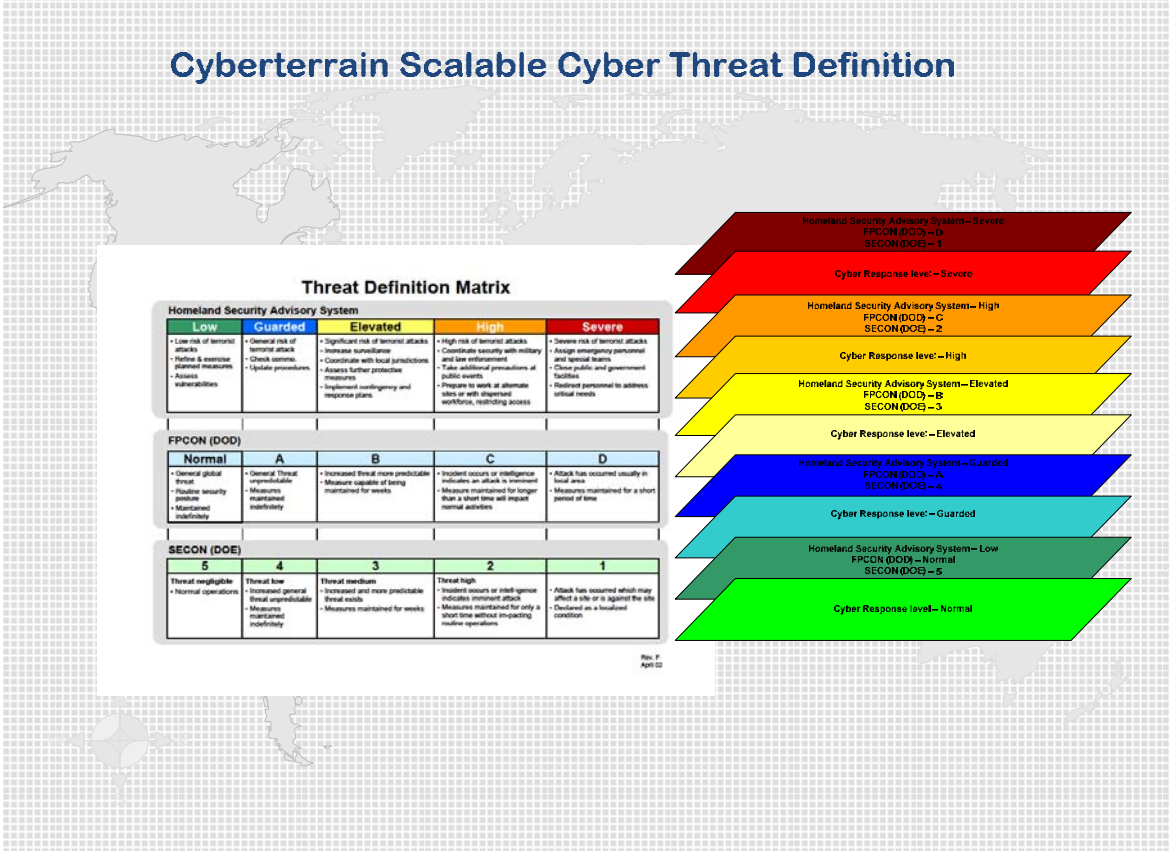


**Figure 18. Conceptual Scalable Cyber Threat Definition**

Conceivably, each layer of the national cyber infrastructure could be protected by five levels of Cyber response, as illustrated in figure 18, resulting in a granular protection scheme across the entire infrastructure.

The fundamental concept is to have five levels of cyber threat definition that match the established levels of physical or kinetic threat definition.

### *5.1.6 Federated Business Continuity Planning Concept of Operations*

The cyberterrain areas of concern pertaining to this concept of operation are:

1. Leadership and Authority
2. Resource Requirements
3. Workforce and Defenders
4. Coordination and Communication

The purpose is a coordinated framework for protection and recovery of critical infrastructure to natural disaster, terrorist attack, kinetic attack, wide-area cyber attack, or other large scale disruption of function and service availability.

The Federated BCP organizational framework adds an information management BCP element for wide-area partner and community of interest (COI) coordination during continuity event operations. The legal and cyber information management aspects are particularly important when handling shared intellectual property, such as with collaborative research agreements, and contractual rapid response requirements for shared or multi-use information systems. It is important that a culture of continuity event awareness is present throughout the organization and with leadership.

It must be safe for people to work before continuity operations begin; this makes Emergency Management the authority to clear BCP activation. Note that communication is central to all recovery operations.

**Federated BCP Command Structure**

Business Continuity Planning (BCP) is a program that assesses the existing operations, risks, and customer relationships of an organization for the development of organizational preparedness. This federated BCP model develops an integrated approach to ensuring that critical processes continue to function during and after a disaster or incident that interrupts the operation of the organization and its business partners. The Homeland Security national incident management system (NIMS) incident command system (ICS) provides the basis for this BCP command structure.

The federated BCP command structure is designed to benefit the operational environment with coordinated emergency management (EM), IT disaster recovery (ITDR), continuity of operations planning (COOP), and collaborative information management (IM). Roles have been assigned as they pertain to executive management and decision makers.

Federated BCP elements are supported through a BCP/COOP program office that is resident in each participating organization. The four elements provide services to keep an organization in operation with contingency for collaborative dependencies during time of crisis. Similarly, the finance and administration functional area has been added because of the critical importance of funds availability during time of crisis. The federated BCP command structure is illustrated in figure 19.

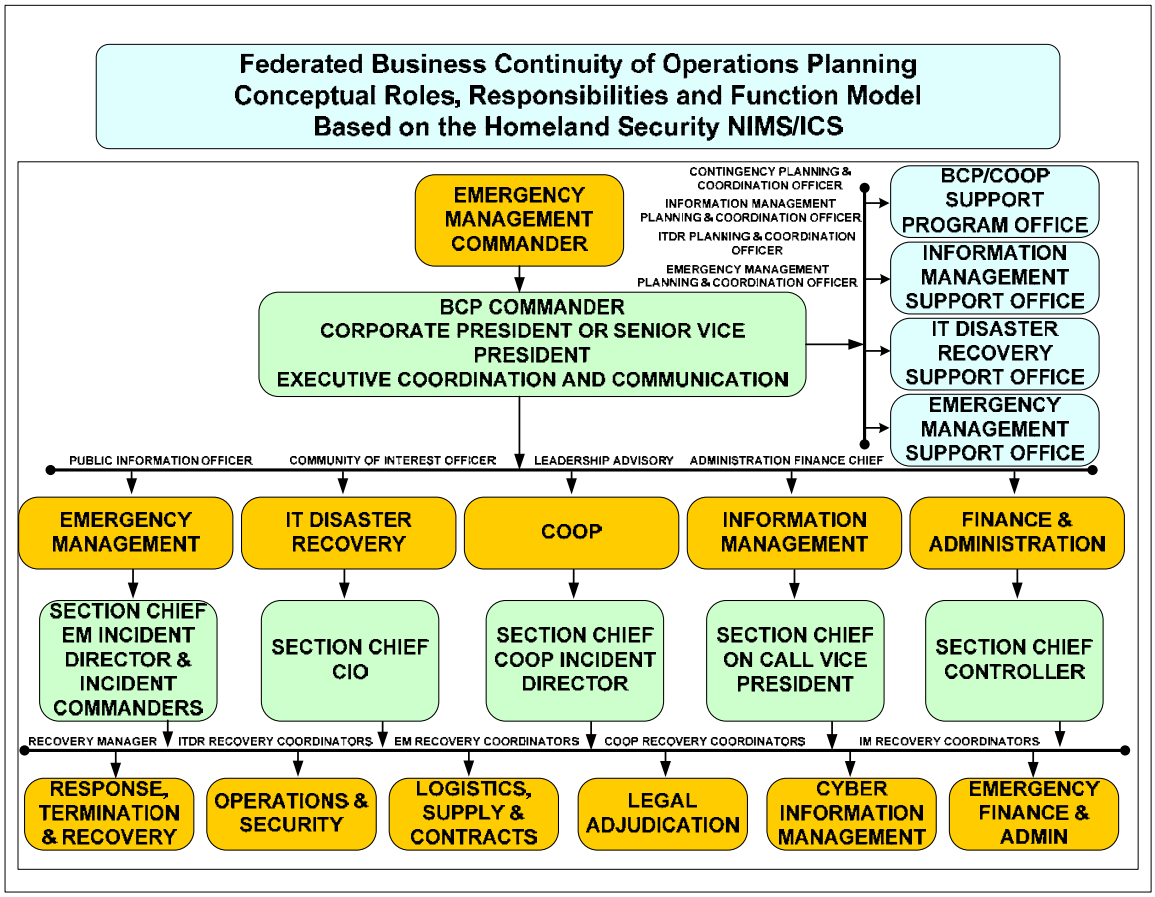


**Figure 19: Federated BCP Command Structure**

Information management is the key BCP element added for the cyberterrain areas of concern. This is necessary to accommodate continuity of operations for interconnected dependencies throughout the national information infrastructure. Also added are new roles to support the BCP information management element, including a community of interest officer (CoIO), and an information management program officer to foster a culture of continuity event awareness throughout each organization and all organizational leadership.

BCP Roles:

- Emergency Management Commander (EMC) - The EMC is responsible for all emergency operations until threats and hazards to people, property and the environment

are terminated. The EMC is a leadership position that owns the responsibility for executive decisions and communications.

- Emergency Incident Director (EID) – The EID is responsible for all emergency operations coordination and communications and doubles as the emergency management section chief. The EID is in place to coordinate multiple IC's during large scale multi-site emergency management events.
- Incident Commander (IC) - An IC is responsible for on-site field emergency operations until threats and hazards to people, property and the environment are terminated. IC's report to the EID and when necessary the EMC.
- BCP Commander (BC) - The BC is responsible for overall BCP coordination and communications. The BC declares BCP activation and termination in coordination with the EMC. The BC is a leadership position that owns the responsibility for executive decisions and communications.
- COOP Incident Director (CID) – The CID is responsible for all COOP operations coordination and communications and doubles as the COOP section chief. The CID is in place to coordinate multiple COOP coordinators across a wide area during large scale multiple site and organization continuity events.
- BCP Planning and Coordination Officer (PCO) – Each COOP, ITDR, EM and IM PCO is responsible for facilitating planning and training activities in times of order and provides coordination across the enterprise and collaborative business partners during BCP activation. PCO's report to the BCP program office and coordinate closely with the PIO, CoIO and members of the leadership advisory. PCO's ensure consistency in development and resources across the organization.
- Public Information Officer (PIO) – The PIO is responsible for public relations communication.
- Community of Interest Officer (CoIO) - The CoIO is responsible for business partner and oversight (USG) communication.
- Leadership Advisory (LA) – The LA is a designated group of corporate officers and section chiefs with the responsibility to provide accurate and timely information to executive leadership. Critical corporate decisions for continuity, sustainability and survivability will rest with the LA.
- Administrative Finance Chief (AFC) – The AFC is responsible for overall coordination of emergency and contingency funding and cost collection.
- Section Chief (SC) – An SC is responsible for coordination of area activities and reporting to the EMC and BC any issues that require higher level attention.
- Recovery Manager (RM) – The RM is responsible for all mission recovery coordination, which includes the restoration of support services needed to perform mission during BCP operations and full recovery to normal operations.
- Recovery Coordinator (RC) - An RC is responsible for supporting the RM by facilitating the resumption and recovery of specific areas of importance (i.e. network, workspace, or cold, warm or hot datacenter recovery activation).

This functional model for federated BCP is considered to be a distributed solution that provides responsiveness to wide-area incidents and allows faster time to solution to interrupted inter-organizational dependencies and problems. The majority of recovery work will be done by operations teams under the direction of the section chiefs. The BCP command structure is

intended to facilitate consistency in approach and communications. Each incident is unique and requires evaluation of vulnerabilities and threats to determine appropriate action. Such a distributed solution will maximize value and provide prepared response to coordinated multisite, multi-method sophisticated attacks.

Figure 20 illustrates the coordination and overlap of EM and BCP facilitated through consistent executive, command, public, internal and external communications where vulnerabilities for each incident are examined. BCP activation is called for by the BC and cleared by the EMC when safe to proceed. When emergency management is not involved the BC assumes full authority of recovery operations. Note that appropriate levels of physical security and cybersecurity must be maintained throughout the BCP life cycle.

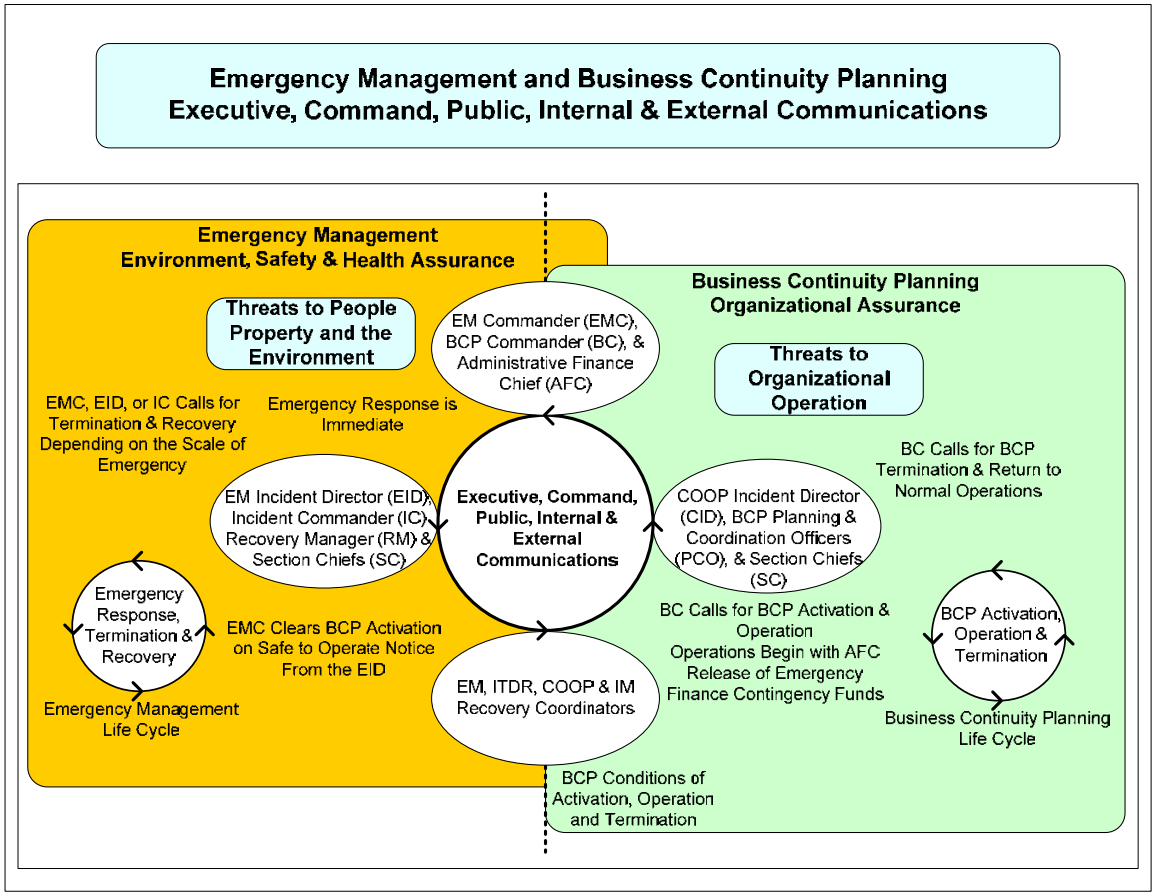


**Figure 20: Emergency Management and BCP Coordination**

**BCP Conditions of Activation, Operation and Termination**

Emergency operations have established methodologies for emergency response rooted in the NIMS / ICS. These include roles and activities that define initial emergency response (activation phase), resolution of the emergency situation (termination phase) and return to normal operations (recovery phase). BCP activation will work in-kind with EM, meaning that the EMC will have authority of control for the BCP activation and operation phases for all operations of the organization. The EID will work with the EMC, the IC's and SC's to manage initial response through to the termination of the emergency situation. The emergency situation is terminated

when threats and hazards to people, property and the environment are controlled and a safe workspace environment is restored. Upon BC declaration of BCP activation, the COOP, ITDR, IM and EM PCO's coordinate BCP operation with the SC's and the recovery teams (recovery manager and recovery coordinators). Executive, command, public, internal and external communications are coordinated with the PIC and CoIO and the BCP program office PCO's.

BCP Conditions of Activation

BCP activation is triggered when an incident is determined to threaten mission operations. Threats to mission operations include: threats to work force personnel, property and the environment requiring emergency response; threats to critical infrastructure that are essential to the operation of the organization (facilities, energy and water utilities, information and communication networks); threats to the operability of critical information assets, processes, supply chain and partnerships.

The BC declares BCP activation to initiate recovery services and communication. BCP activation puts into action mission operation contingency plans in order to sustain critical processes and services with the release of contingency funds availability from the AFC. The BC works in coordination with the EMC when emergency management is necessary to restore a safe working environment. When the safety to people, property or the environment is threatened the EMC assumes authority for recovery operations. Otherwise the BC assumes full authority of recovery operations.

BCP Conditions of Operation

BCP operations initiate upon BCP activation as contingency plans and recovery operations begin. Contingency operations run in conjunction with EM recovery operations through to completion of the BCP operations phase. Mission recovery includes the recovery of facilities, infrastructure and services required for the return to normal operations. It is important that detection and investigation and risk management activities continue throughout BCP activation. The BC declares that BCP operations are completed upon consensus from the EMC, LA, and executive leadership.

BCP Conditions of Termination

BCP operations can be terminated when facilities, infrastructure and services are sustainable and reliable. The BC declares that normal operations may resume upon consensus from the EMC, LA, and executive leadership. The AFC closes contingency funds availability upon return to normal operations and commences financial reconciliation activities.

Critical BCP Issues:

BCP operations are dependent on planning, communication, coordination and security. Critical issues include:

1. Personnel Safety
2. Environmental Safety
3. Physical Security
4. Cybersecurity
5. Continued Detection, Investigation and Risk Management
6. Identification of Critical Personnel
7. Identification of Critical Physical Assets
8. Identification of Critical Communities of Interest
9. Identification of Critical Information Assets
10. Identification of Critical Processes
11. Identification of Vital Records
12. Established Command Structure
13. Managed Command Communications
14. Managed Public Information and Safety Communications
15. Managed EM and BCP Internal Communications
16. Managed EM and BCP External Communications
17. Prioritization of Activities
18. Training, Testing and Continual Improvement
19. Timely Leadership Communications
20. Managed Work Force and Defender Communications
21. Managed Telecommute Work Force Information and Communications
22. Managed External Partner and Oversight Information and Communications
23. Managed Legal Adjudication and Information Protection
24. Managed Contractual Obligations

### *5.1.7 Solution Space Concepts of Operation: Assessment Conclusions*

1. A variety of concepts of operations can be applied in the wide-area design space to address the scope of a national cyber defense capability.

2. Expansion of extant enterprise security, configuration management, and service architectures can be applied for staged preparedness and defense in the face of escalating threat.

3. A comprehensive wide area coordinated response solution comprises many disciplines and several methods designed to function in unison.

## 5.2 Roadmap with Quantifiable Goals and Objectives

Goal: *Develop next steps and outline a roadmap for progressive development of Wide-Area Cyber HPC Analysis with quantifiable goals and objectives.*

People and purpose underpin the need for secure information processing. People drive innovation, which drives purpose, such as modeling and simulation, which in turn provides opportunities for technology to contribute to better quality of life.

Science and technology represent the basis of the national cyber dilemma and the foundation for cybersecurity in the wide-area cyberterrain. However, cybersecurity is much more than technical in nature; it is also social and cultural. HPC analysis of the cybersecurity problem domain permits exploration and understanding of these complexities in an overall system of system context, as an ecosystem.

There is need for a shift in the way we consider function and security, whereby security becomes a critical design criterion. Secure software development, cybersecurity coupled systems engineering, and trusted systems platforms and communications infrastructure are not widely

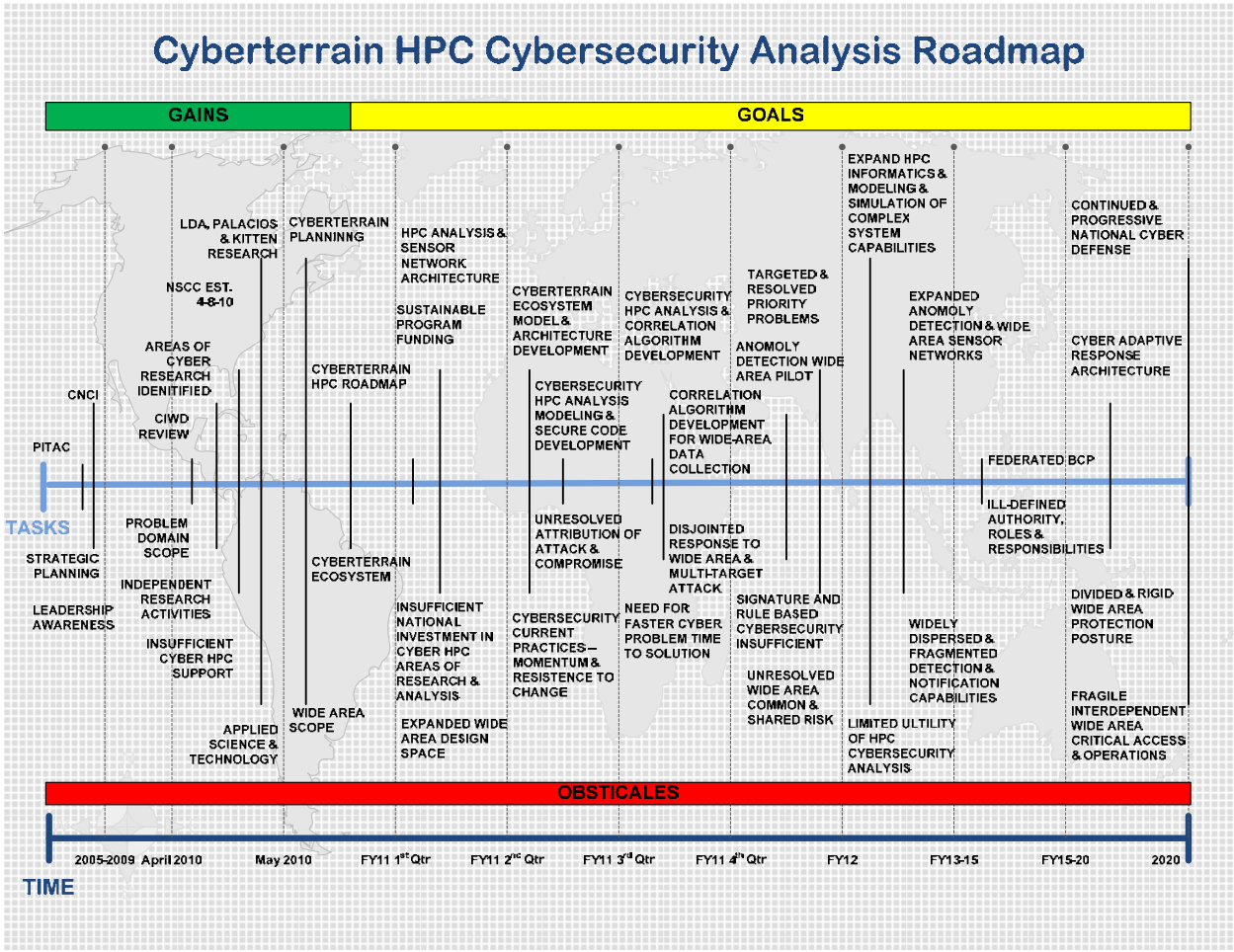


**Figure 21: Cyberterrain HPC Cybersecurity Analysis Roadmap**

practiced or available today. These fundamental aspects of security in the cyberterrain must change to enable an effective national cyber defense capability.

Quantifiable Goals:

1. Sustainable Program Funding
2. HPC Analysis and Sensor Network Architecture
3. Cyberterrain Ecosystem and Model Architecture Development
4. Cybersecurity HPC Analysis Modeling and Secure Code Development
5. Cybersecurity HPC Analysis and Correlation Algorithm Development
6. Correlation Algorithm Development For Wide-Area Data Collection
7. Anomaly Detection Wide-Area Pilot
8. Targeted and Resolved Priority Problems
9. Expand HPC Informatics and Modeling and Simulation of Complex System Capabilities
10. Expanded Anomaly Detection and Wide-Area Sensor Networks
11. Federated Business Continuity Planning
12. Cyber Adaptive Response Architecture
13. Continued and Progressive National Cyber Defense

This roadmap encompasses a collaborative scope for solutions in the wide-area cyberterrain and presents a path forward to comprehensive national cyber defense through the utility of HPC capability. Long range goals for continued and progressive national cyber defense include the possible outcomes and actionable results illustrated in figure 22.

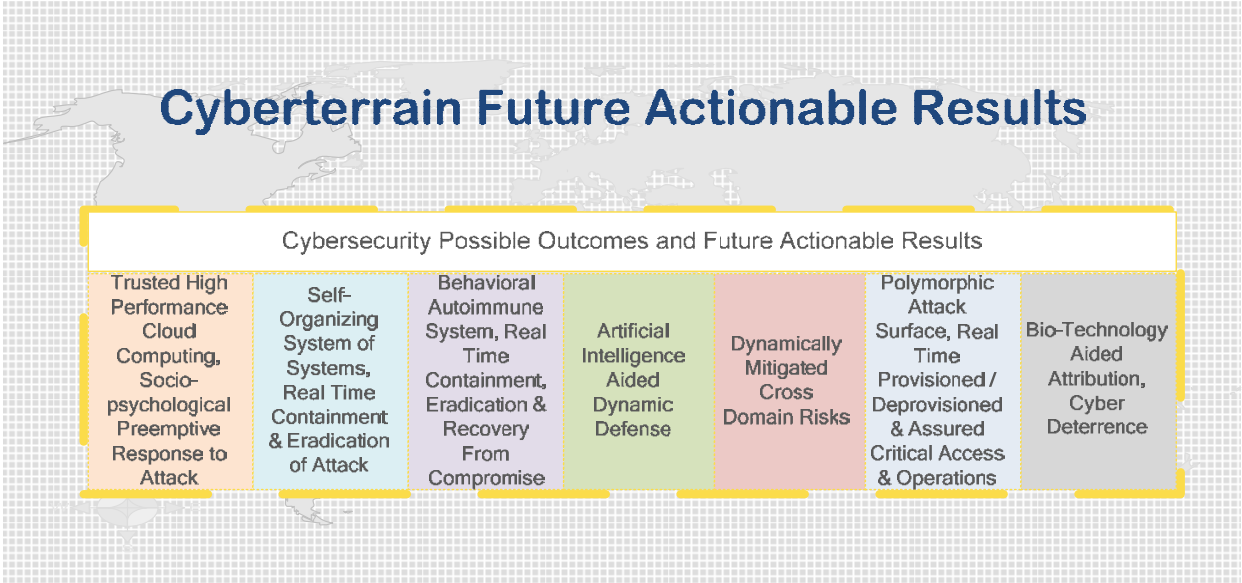


**Figure 22: Cyberterrain Possible Outcomes and Future Actionable Results**

Quantifiable Objectives:

**Table 5. National Cyber Defense Quantifiable Objectives**

| | | | | |
|---|---|---|---|---|
| Inform the Decision Maker | Inform the Defender | Minimize Exposure | Reduce the Attack Surface | Effective Defense |
| Degree of Coordination | Degree of Unity | Degree of Investment | Degree of Resilience | Degree of Commitment |

Figure 23 illustrates that a combination of complexity science and modeling and simulation of large scale networks might result in an improved understanding of networked systems. This understanding could be used to produce more effective correlation and graph analysis algorithms, which could in turn be used, for example, to determine choke points in the network that would be most effective for quarantining attack or for enforcing a selective reduction in service to slow the spread of attacks. This would help realize our goals of a minimized attack surface, assured critical access and operations, and an adaptive and agile defense. The improved understanding of networked systems might also lead to signatures and predictors of attacks and information compromise, which would locally enhance near real-time notification of information compromise and improve notification of infrastructure attack in the wide-area.

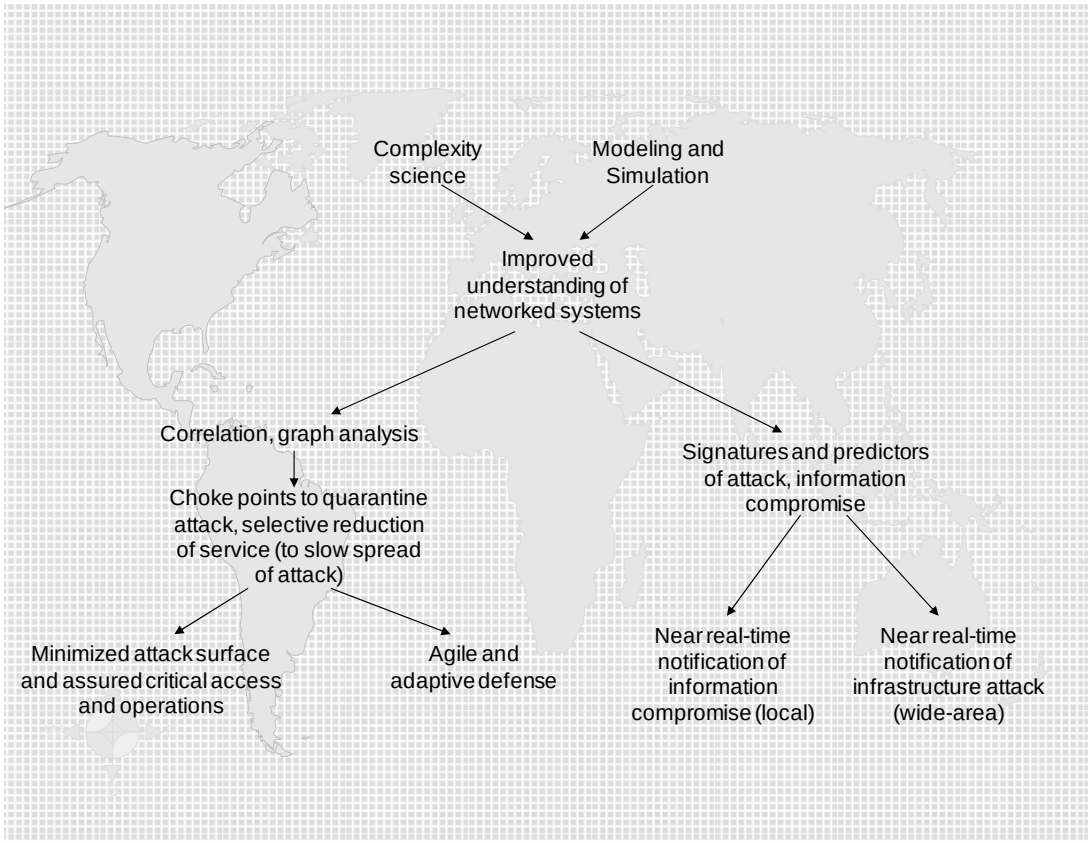


**Figure 23: HPC Complexity Analysis and Modeling & Simulation Desired Outcomes**

Figure 24 shows that notification of information compromise would also be enhanced by combining TICs and distributed cybersecurity sensor networks with research in informatics, statistics, correlation algorithms, and data filtering.

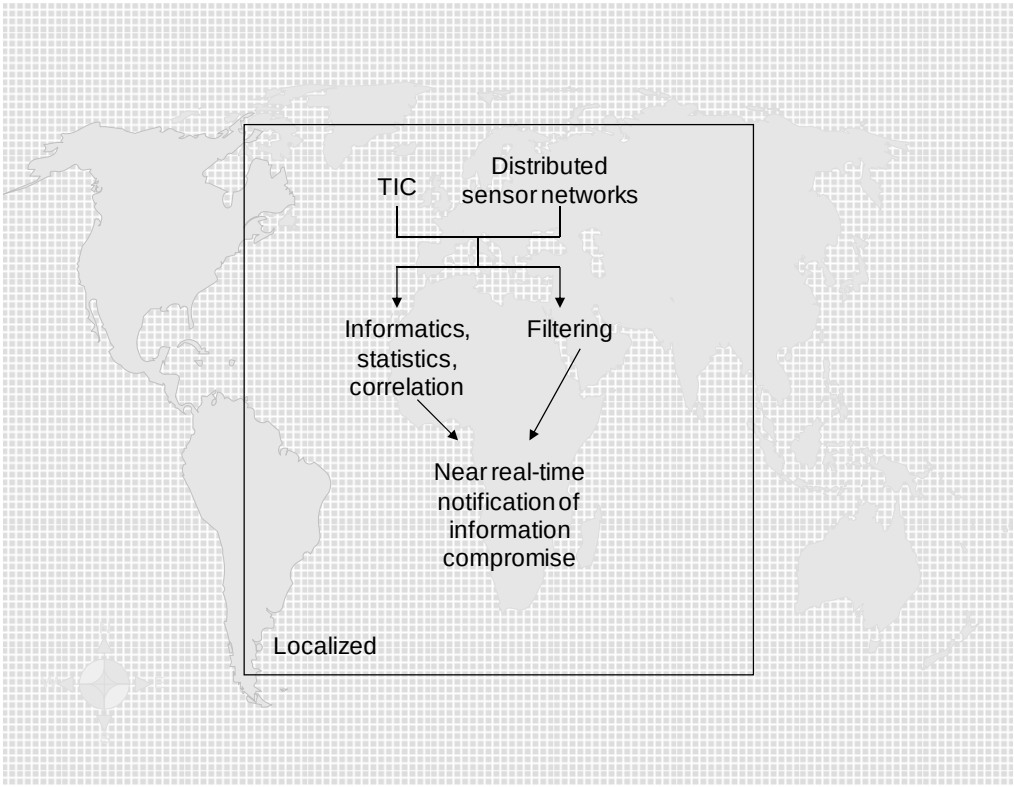


**Figure 24: Localized Trusted Interface Connections Desired Outcomes**

Identification and response to attack may be improved by combining the data collected at TICs with data aggregation, informatics and statistics to produce datasets appropriate for HPC correlation and analysis algorithms, as illustrated in Figure 25.

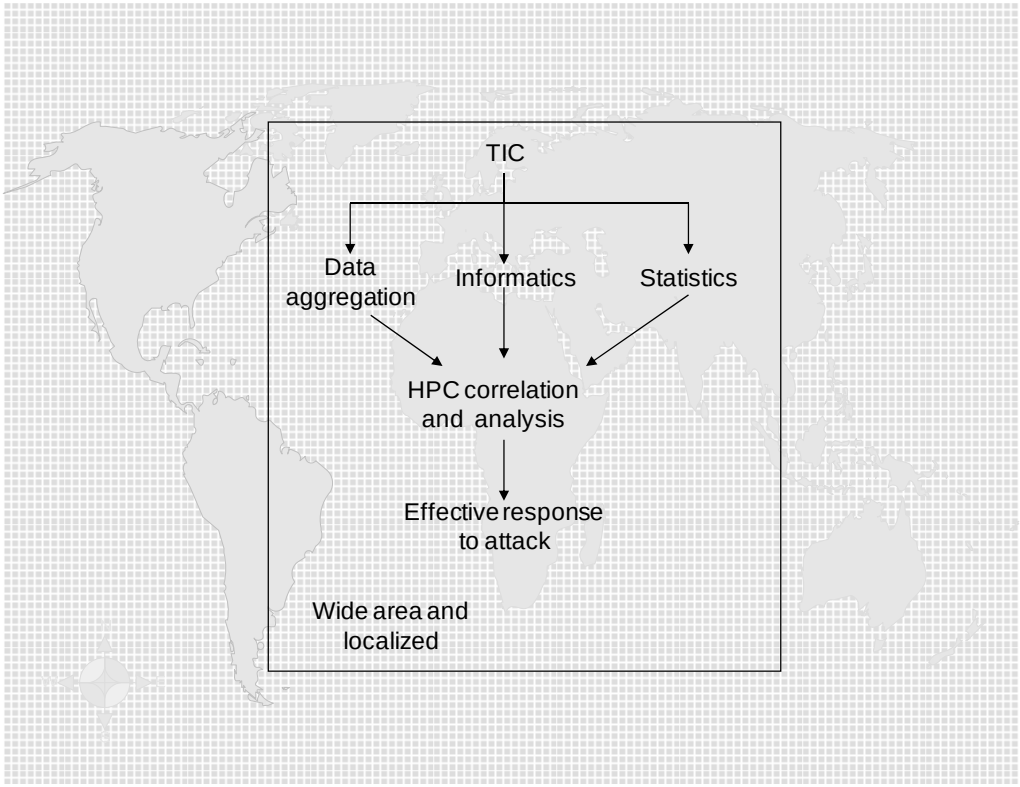


**Figure 25: Wide Area and Localized Trusted Interface Connections Desired Outcomes**

Figure 26 further illustrates the benefit of a comprehensive planning approach that encompasses identifying shared risks and deploying broad risk mitigations to meet shared goals in national cyber defense.

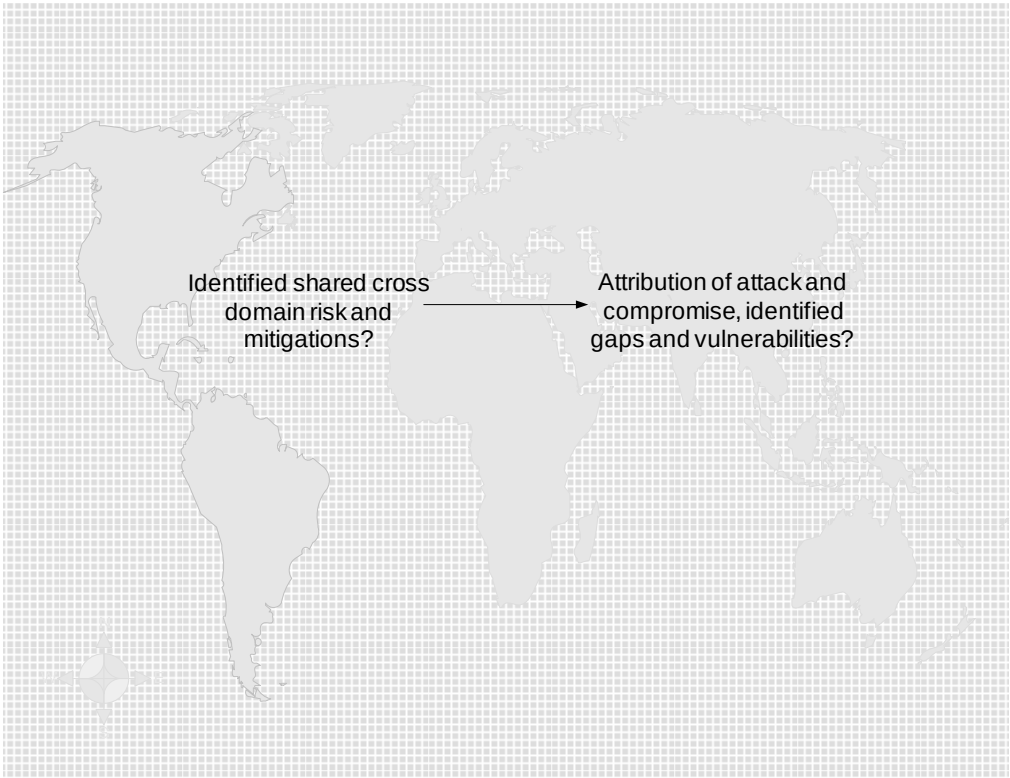


**Figure 26: Identified Shared Risk and Mitigations Desired Outcomes**

A collection of roadmaps such as these may help prioritize research around those areas found to have the greatest impact or most wide-spread applicability. There is much more to be done that requires coordination and commitment to achieve the broad vision discussed here. The challenges are many and cybersecurity HPC analysis presents a means to jumpstart a national scale cyber defense effort.

We find that cybersecurity HPC analysis is a catalyst to achieving comprehensive national cyber defense as a fundamental means to study and understand the multifaceted complexities in a wide-area design and solution space comprising complex technical, organizational and human systems.

# 6. CHALLENGES, OPPORTUNITIES, AND CONCLUSIONS

## 6.1 National Cyber Defense Challenges

We've selected ten national cyber defense challenges derived from each phase of assessment.

1. Cyber deterrence is ineffective without a means to identify the level of sophistication and who is responsible for attack.

2. The study and understanding of technical, organizational and human complexity within the wide-area national information infrastructure is beyond human comprehension without the utility of supercomputing.

3. Critically important to national cyber defense is the coordination and work toward shared goals to address shared risks and therefore an effective defense to wide-area or sophisticated multi-stage attack.

4. The composition and complexity of national information infrastructure cybersecurity with connectivity to the global Internet is commensurate to a multi-cultural human, organizational, legal and technical ecosystem.

5. Culture and technology are intertwined as technology is exercised at the discretion of human directive.

6. Distributed sensor networks and HPC cybersecurity analysis need to be considered together as one system of data collection, analysis and response to account for data locality, transport, throughput, latency, processing time and return of information to defenders and defense devices.

7. A full spectrum or holistic approach is needed to address the broad scope of an environment on the scale of the national information infrastructure.

8. An increased investment in terms of time, resources and funding in secure software development and validation, and trusted hardware as codependent requirements is needed for national cyber defense advancements.

9. Progress for the advancement of the national cyber defense posture is severely inhibited without strong executive leadership, organizational commitment, multi-agency program support, and increased funds availability.

10. A comprehensive wide area coordinated response solution comprises many disciplines and methods that must function in unison.

## 6.2 Ten High Impact Opportunities

We've selected ten high impact opportunities derived from each phase of assessment.

1. Cybersecurity HPC analysis is a potentially game changing means to support a wide-area rapid time-to-solution national cyber defense capability.

2. Modeling and simulation of very large complex systems may reduce cost and time-to-deployment of wide-area national cyber defense technologies.

3. Potential LDA anomaly detection advantages include zero day detection at initial act of exfiltration.

4. LDA anomaly detection can be extended to a formal risk-based approach with faster time-to-resolution and high value cyber deterrence benefits.

5. Investment in the HPC areas of research, the identified areas of impact and the actionable results can facilitate PITAC cybersecurity research priorities.

6. The knowledge gained through HPC analysis and evaluation may prove vital for economic, civil, and national security assurance.

7. Conceptually, I&AM, PBNM and SOA can be extended to Behavior Based Entitlement Provisioning, Situational Staged Defense Posture, and Threat Case or Rapid Response Virtualized SOA as a means of managing the primary attack surfaces available to an adversary.

8. The integration of modeling and simulation with live interactive networks offers an arena for the evaluation of emerging cyber-threats and the validation of national cyber-defense mission capability to recover from attack.

9. Conceptually, distributed high-speed sensor networks and cluster, commodity or hybrid HPC systems, which are co-located or in close proximity to the data source, could perform near real-time fast I/O HPC accelerated processing.

10. A variety of concepts of operations can be applied in the wide-area design space to address the scope of a national cyber defense capability.

## 6.3 National Cyber Defense HPC Analysis Concepts, Planning and Roadmap: Conclusions

1. As a society we share cyber risks to interconnected information systems and therefore share a set of common goals for a more secure national information infrastructure.

2. Cybersecurity HPC analysis is a catalyst to achieving comprehensive national cyber defense as a fundamental means to study and understand the multifaceted complexities in a cyberterrain comprising complex technical, organizational and human systems.

3. Distributed data collection and future petascale and exascale supercomputing analysis are anticipated requirements to adequately address a national cyber dilemma of increasing complexity.

4. Leadership, investment and coordination are needed for the successful and continued development of advanced HPC cybersecurity analysis and the development of next generation national cyber defense.

5. HPC analysis of cybersecurity in the national information infrastructure provides the strategic means to: understand your adversary; understand the interdependencies and interaction of technical and cultural behaviors; and enable movement from reactive to anticipatory and predictive national cyber defense.

6. Sandia National Laboratories has an opportunity to collaboratively serve the national interest to resolve national cybersecurity issues through inter-organizational program development with multiple USG sponsors, State, County, Municipal, American Indian Tribal Governments, and industry and academic partners.

We conclude that a national call to arms is on order to fulfill the national cyber defense mission.

# DISTRIBUTION

| | | | |
|---|---|---|---|
| 1 | MS0321 | Robert W. Leland | 1400 |
| 1 | MS1221 | James S. Peery | 5600 |
| 1 | MS0801 | Tom Klitsner | 9300 |
| 1 | MS1231 | Ann N. Campbell | 1950 |
| 1 | MS0620 | Edward J. Nava | 5620 |
| 1 | MS0620 | Mark G. Terhune | 5630 |
| 1 | MS0620 | Rebecca Darnell Horton | 5640 |
| 1 | MS0823 | John D. Zepper | 9320 |
| 1 | MS0838 | G. Kelly Rogers | 9330 |
| 1 | MS1318 | Vitus J. Leung | 1415 |
| 1 | MS1318 | David G. Robinson | 1415 |
| 1 | MS1319 | Suzanne M. Kelly | 1423 |
| 1 | MS1319 | Kevin Pedretti | 1423 |
| 1 | MS0672 | David P. Duggan | 5621 |
| 1 | MS0671 | Fredrick M. McCrory | 5627 |
| 1 | MS0671 | Tan (Richard) Chang Hu | 5627 |
| 2 | MS0672 | Jason R. Hamlet | 5627 |
| 1 | MS9158 | Keith Vanderveen | 8961 |
| 1 | MS0823 | William R. Claycomb | 9326 |
| 1 | MS0807 | John P. Noe | 9328 |
| 1 | MS0807 | Robert A Ballance | 9328 |
| 1 | MS0823 | Geoffrey (Geoff) F. McGirt | 9328 |
| 1 | MS0806 | Timothy (Tim) M. Berg | 9336 |
| 1 | MS0806 | Anand Ganti | 9336 |
| 1 | MS0806 | Steve A. Gossage | 9336 |
| 2 | MS0806 | Curtis M. Keliiaa | 9336 |
| 1 | MS0806 | John H. Naegle | 9336 |
| 1 | MS0806 | Marie-Elena (Laney) Kidd | 9336 |
| 1 | MS0806 | Jimmie V. Wolf | 9336 |
| 1 | MS0932 | Timothy L. MacAlpine | 9514 |
| 1 | MS0899 | Technical Library | 9536 (electronic copy) |

Sandia National Laboratories