Funding Innovative Network and Cybersecurity Research

Anita Nikolich
National Science Foundation
Program Director, Advanced Cyberinfrastructure
May 2015

NSF Core Mission: Fundamental Research

$7.7 billion FY 2016 research budget

94% funds research, education and related activities

50,000 proposals

11,000 awards funded

2,000 NSF-funded institutions

300,000 NSF-supported researchers

Fundamental Research

Trends and Challenges for (US) Research

- Changing practice of science: interdisciplinary, team-oriented, global, data intensive, complex work and data flows increasingly integrated with technology
- The power and opportunity of technology: instrumenting everything; computational and data learning and workforce development; ubiquitous connectivity
- Shifting funding landscape and role for foundational research in the face of escalating global challenges
- Changing demographics: diversity, increased need for more computational and data scientists

Computer and Information Science and Engineering (CISE) Directorate

Exploring the frontiers of computing

- Promote progress of computer and information science and engineering research and education, and advance the development and use of cyberinfrastructure.
- Promote understanding of the principles and uses of advanced computer, communications, and information systems in support of societal priorities.
- Contribute to universal, transparent and affordable participation in a knowledge-based society.

These frontiers have interfaces with all the sciences, engineering, education and humanities and a strong emphasis on innovation for society.

Computing frontiers, national priorities

From Data to Knowledge to Action

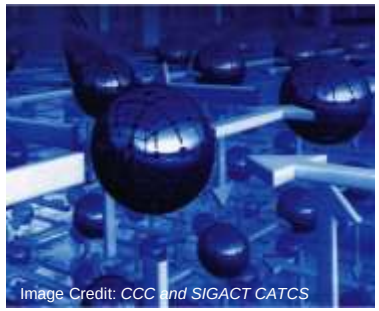
Manufacturing, Robotics, & Smart Systems

Understanding the Brain

Secure Cyberspace

Education, Workforce Development

Augmenting Human Capabilities



Expanding the limits of computation

Cognitive Science and Neuroscience

Goal: Understanding the human brain

- White House BRAIN Initiative launched in April 2013 (NSF, NIH, DARPA).
- Addresses critical challenge of research integration across multiple scales ranging from molecular to behavioral levels.
- Builds on NSF's unique ability to catalyze multi-disciplinary research and ongoing NSF investments.
  - Cyberinfrastructure
  - National Brain Observatory

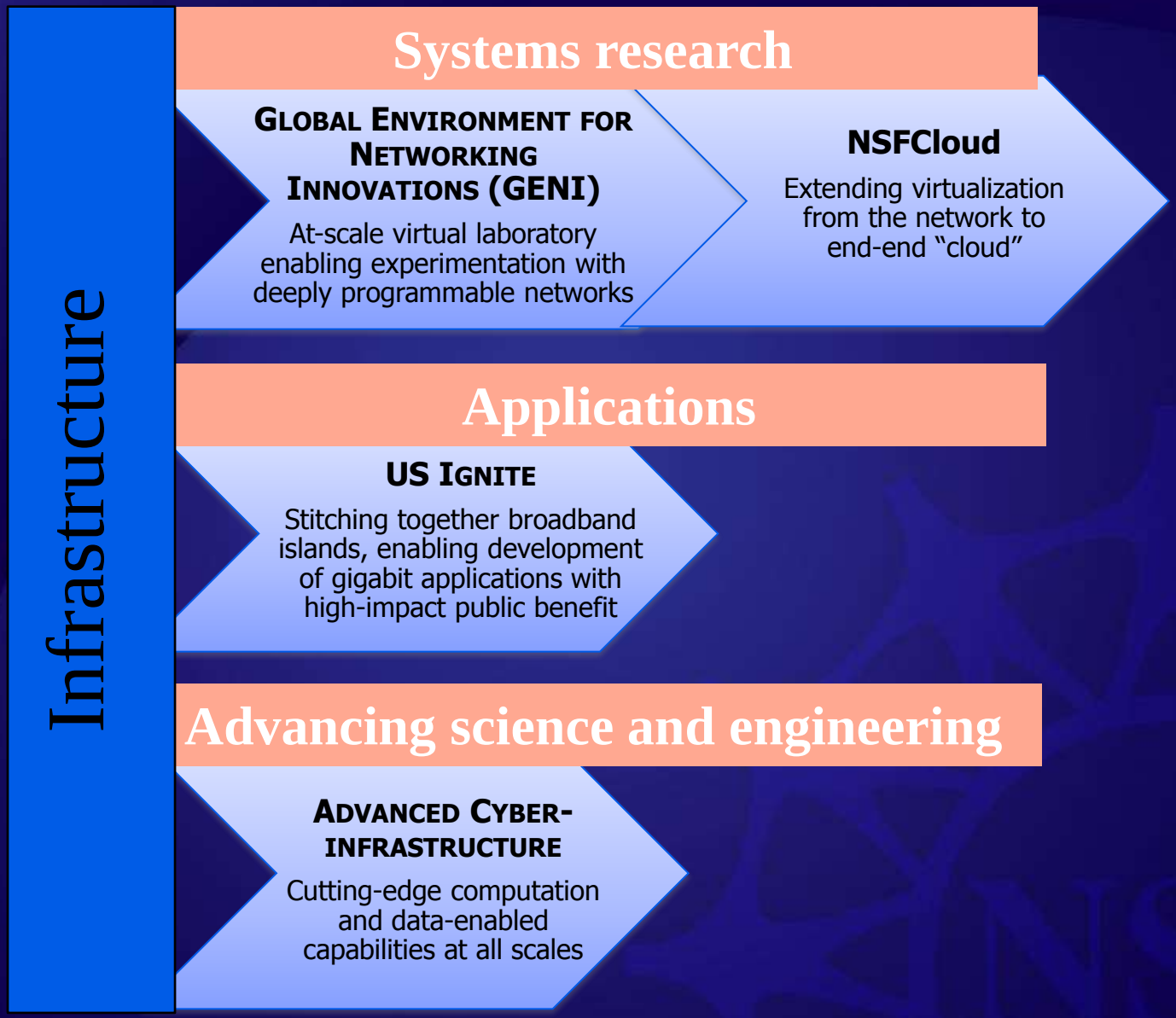
- **Multiscale & Multimodal Modeling** to relate dynamic brain activity to behavior
- **Comparative Analyses Across Species** to identify conserved functional circuitry: take advantage of Biodiversity
- **Innovative Technologies** to understand brain function and treat brain disorders
- **Cyber Tools & Standards** for data acquisition, analysis and integration
- **Quantitative & Predictive Theories** of brain function

Innovations at the Nexus of Food, Energy, and Water Systems (INFEWS)

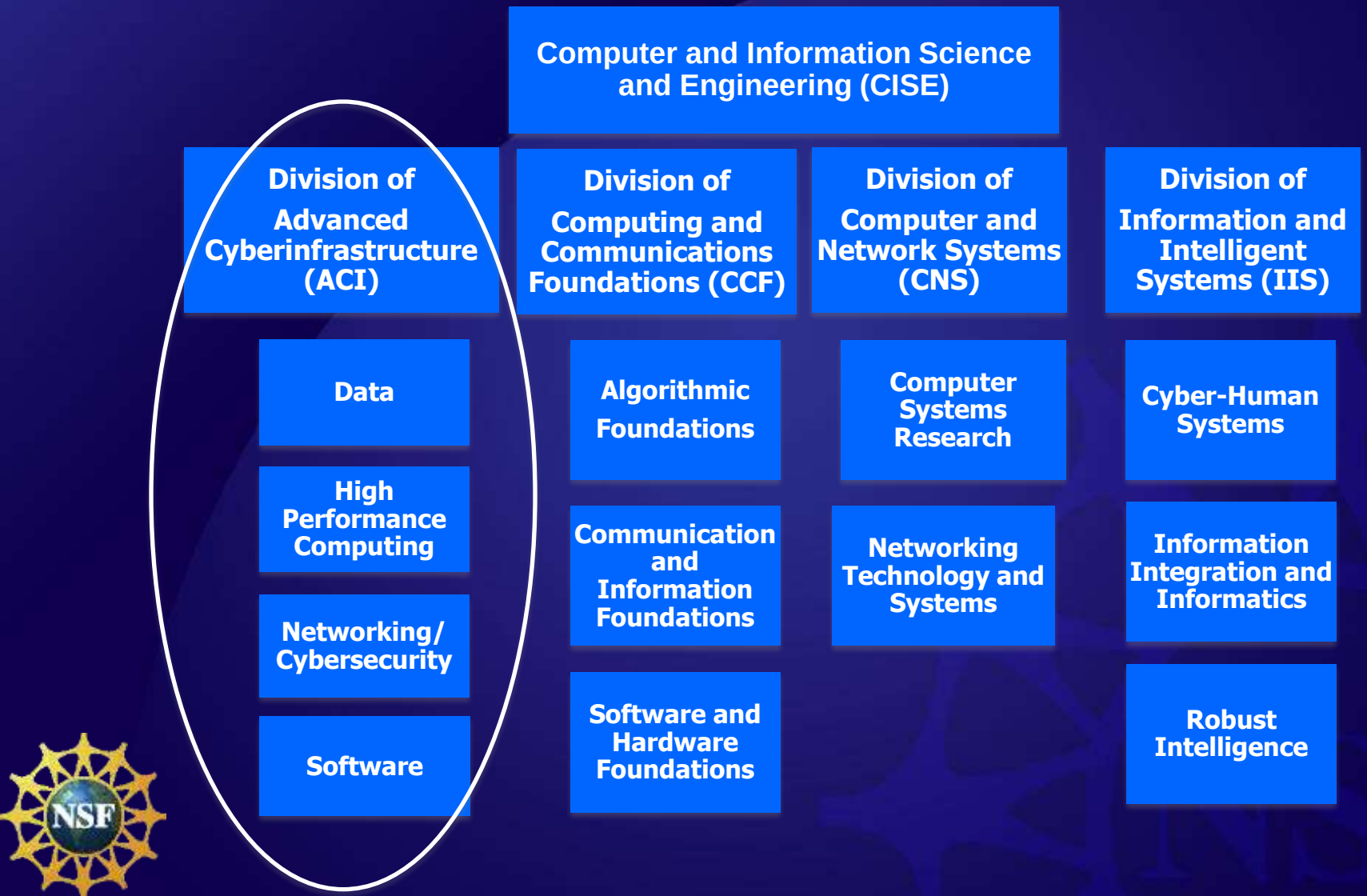
Securing and protecting food, energy and water resources

- Partnership among all NSF directorates
  - New resource management algorithms, architectures
  - Real-time coordination, communications
  - Robust observation, sensing, inference
  - Large-scale data analysis/management, including modeling, simulation
  - Optimization of complex systems
  - Advancing computational infrastructure

GENI: At-scale Network Experimentation



NSF Advanced Cyberinfrastructure (ACI) is part of the CISE Directorate



Advanced Cyberinfrastructure (ACI)

Supports the research, development, acquisition and provision of state-of-the-art CI resources, tools, and services:

- ***High Performance Computing**:* Provide open-science community with state-of-the-art HPC assets ranging from loosely coupled clusters to large scale instruments; develop a collaborative and innovative scientific HPC environment.
- ***Data:*** Support scientific communities in the use, sharing and archiving of data by creating building blocks to address community needs in data infrastructure.
- ***Networking and Cybersecurity**:* Invest in campus network improvements and re-engineering to support a range of activities in modern computational science. Support transition of cybersecurity research to practice.
- ***Software:*** Transform innovations in research and education into sustained software resources (shared tools and services) that are an integral part of cyberinfrastructure.

HPC:
Blue Waters: Grand Challenge Computational Science and Engineering through Sustained Petascale Performance

UIUC Data Center

Cray XE6/XK7 accepted December, 2012

Petascale Application Projects

May, 2013

Credit: *Theoretical and Computational Biophysics Group (www.ks.uiuc.edu), Beckman Institute for Advanced Science and Technology, UIUC*

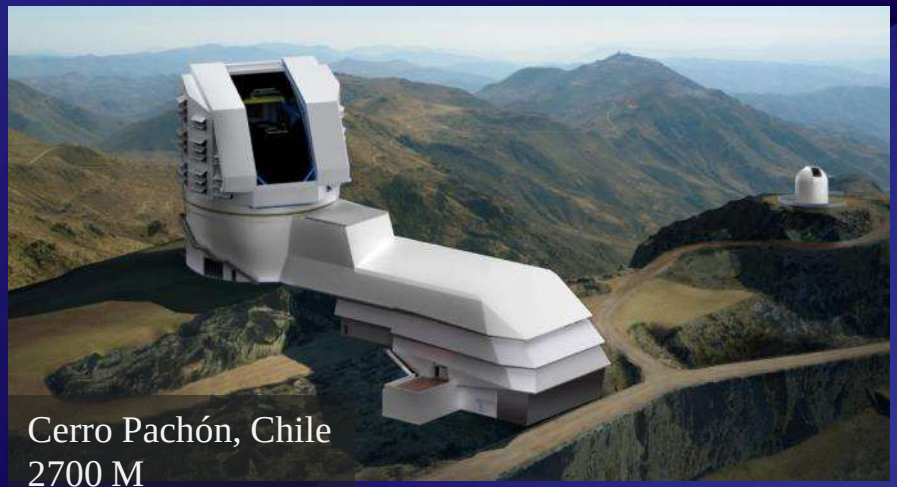
National Ecological Observatory Network (NEON)

The first integrated platform for discovery of change dynamics in the biosphere on regional to continental scales

Open Data Enabled Science:

- 12,000 atmospheric, ground & stream sensors, and organismal sampling across **106 U.S. sites**
- Airborne site-flyover program combining lidar, spectrocopy and optical imaging
- Standardized, continually re-calibrated measurements and automated data QA/QC
- **~700 streaming Data Products** (~40 TB data/yr) will be available on the NEON Portal. Physical samples available to the research community.

Large Synoptic Survey Telescope (LSST)



A survey of 20 billion objects in space and time

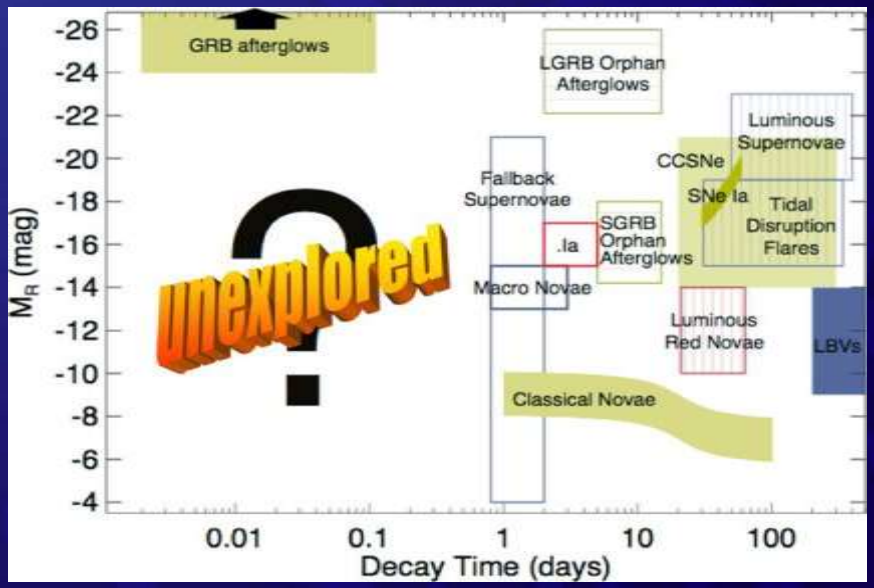
- ***Probe Dark Matter & Dark Energy***
- ***Map the Milky Way Galaxy***
- ***Catalog Solar System Objects***
- ***Detect Transient Phenomena***

- Open Data Enabled Science:
  High dimensional data exploration

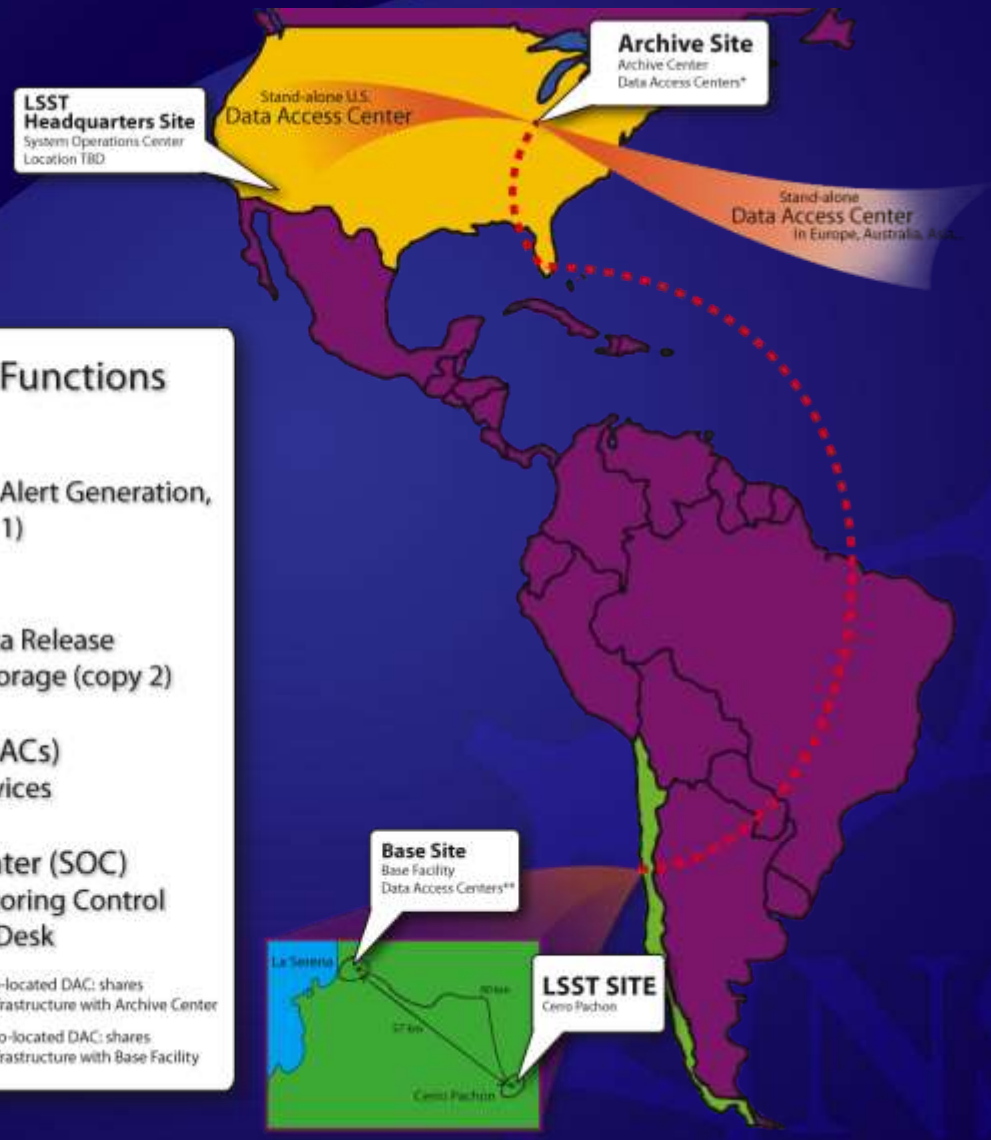
  Very large datasets allow for precision statistical analysis and automated rare and transient event detection

- Massively parallel astrophysics

  A new window on the Universe to "expect the unexpected" will transform astronomical research culture and practice



Nightly transfer rates of 20-40 Tb. LSST network will use 2x100Gbps fiber from summit to base site (La Serena,Chilean Data Access Center), and then 2x40Gbps fiber to US/NCSA (Champaign-Urbana)



Site Roles and their Functions

- **Base Facility**
  Real-time Processing and Alert Generation, Long-term storage (copy 1)
- **Archive Center**
  Nightly Reprocessing, Data Release Processing, Long-term Storage (copy 2)
- **Data Access Centers (DACs)**
  Data Access and User Services
- **System Operations Center (SOC)**
  System Supervisory Monitoring Control & End User Support/Help Desk

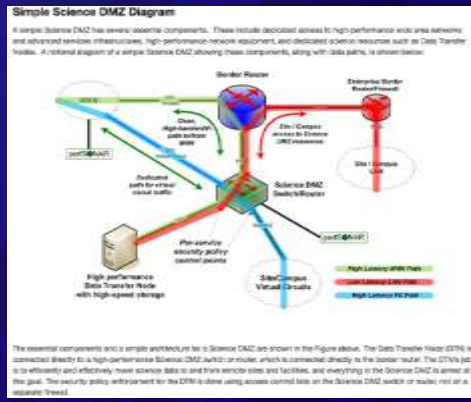
* Co-located DAC: shares infrastructure with Archive Center

** Co-located DAC: shares infrastructure with Base Facility

Networking Programs in CISE/ACI

Networking as a fundamental layer and underpinning of Scientific Cyberinfrastructure

- CC*DNI (Campus Cyberinfrastructure – Data, Networking and Innovation
  - Campus networking upgrade (re-design to scienceDMZ at campus border and 10/100Gbps) and innovation program
- IRNC – International R&E Network
  - Scientific discovery as a global collaborative endeavor
  - Provide network connections linking U.S. research with peer networks in other parts of the world
  - Stimulate the deployment and operational understanding of emerging network technology and standards in an international context
  - 100Gbps trans-oceanic experimental trials underway



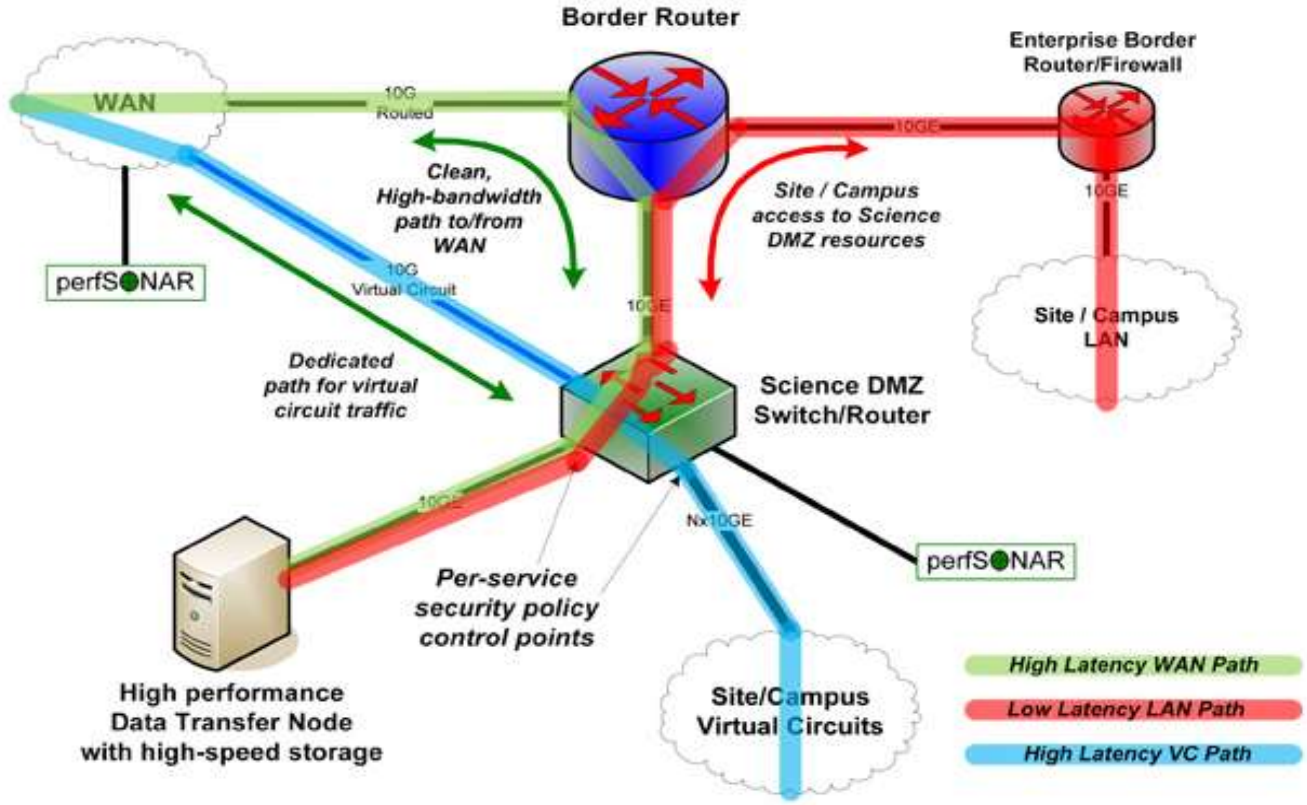
Examples of Funded Network Activities

- Re-architecting a campus network to support large science data flows, for example by designing and building a "**science DMZ**"
- Integration of networking protocols/technologies with application layer
- Transitioning successful research prototypes in SDN, and activities supported by GENI and FIA programs, to distributed scientific environments and campus infrastructure
- Innovative network solutions to problems driven by distributed computing and storage systems including cloud services.
- Federation-based security solutions for dynamic network services extending end-to-end
- Network connection upgrade (10/40/100 Gb) for the campus connection to a regional optical exchange or point-of-presence that connects to Internet2 or National Lambda Rail.
- 10-100Gbps connectivity to/from Asia and Americas
- Open Exchange Points in US
- Primary NOC
- Advanced Network Measurement

The Science DMZ

Simple Science DMZ Diagram

A simple Science DMZ has several essential components. These include dedicated access to high-performance wide area networks and advanced services infrastructures, high-performance network equipment, and dedicated science resources such as Data Transfer Nodes. A notional diagram of a simple Science DMZ showing these components, along with data paths, is shown below:



The essential components and a simple architecture for a Science DMZ are shown in the Figure above. The Data Transfer Node (DTN) is connected directly to a high-performance Science DMZ switch or router, which is connected directly to the border router. The DTN's job is to efficiently and effectively move science data to and from remote sites and facilities, and everything in the Science DMZ is aimed at this goal. The security policy enforcement for the DTN is done using access control lists on the Science DMZ switch or router, not on a separate firewall.

CC*IIE Award Map 2012-2014

Example Science Drivers from ACI Networking Programs

- UMaryland – developing network embedded storage and compute resources via Software Defined Networking (SDN) and exposing services to **scientific applications and workflows**
- UWashington – campus networking upgrades doubled **particle physics** data transfers to/from PNNL to 1.4Gbps single flow (Ed Lazowska, PI)
- 4X capacity improvement (80Gbps aggregate) in connecting **Astronomy** facilities in Hawaii to US mainland
- 4X capacity improvement (40 Gbps aggregate) between US and South America – **LSST** may require 100Gbps by 2020

University of Dayton

- Impact– "a high performance connection…driven by our NSF strategy of providing DMZ connections for researchers with a specific need. NSF is truly helping the University of Dayton 'raise the entire harbor' for science and engineering work on campus and we have used the prestige of this grant to get the attention of our campus leadership to ensure the continued funding for HPC investments.
- Impact on Dayton Partners - "Our work bringing up the connections at Central State Univ (Historically Black College) has gone well. Part of our funding supports upgrades at their campus. CSU does not have deep-expertise on networking at their campus, so we sent our engineering staff to supervise the work of contractors in upgrading their fiber and connecting the new DMZ infrastructure…the NSF support has truly transformed a chunk of the CSU network into a **science-ready environment** that has our researchers **working collaboratively** with their faculty and students. The funding from NSF is making a huge difference for several faculty and students at Central State - They are working on cutting edge projects with Vijay Asari on our campus in the area of "Computer Vision"

Thomas Skill, PI (CIO) University of Dayton

University of Houston Upgrade of Regional Capacity to 100Gbps

- "This expands the effected student base and researchers by multiple orders of magnitude. In fact, Baylor College of Medicine alone sometimes may require sustained ~5 Gbps upload processes that may go on for a few days at this time. Their **genome researchers** and other biomedical researchers are leaders in the nation. The other institutions include: MD Anderson Cancer Center, Houston Museum of Natural Science, University of Texas – Health Sciences Campus, and so on.
- The network refresh has revamped the SETG organization to refresh their technical advisory group, decision processes, and future investment perspectives in supporting research in network science and engineering as well as better support of science data flows with more transparency and control."

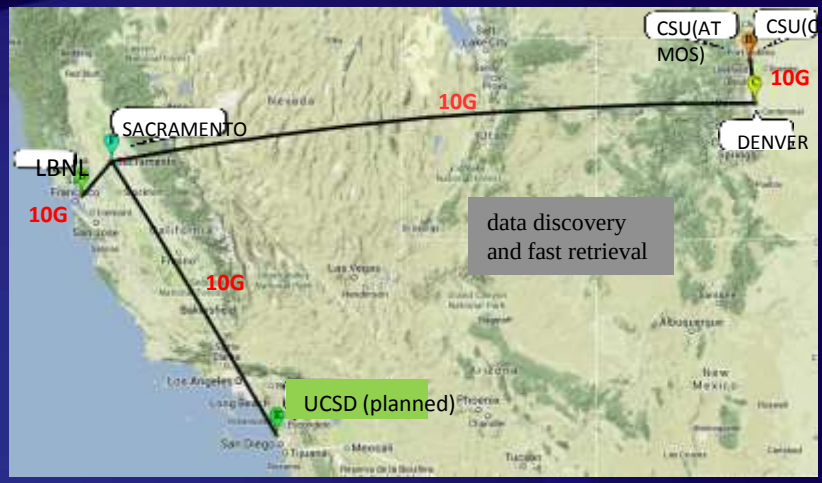
– Deniz Gurkan, PI, Univ. of Houston

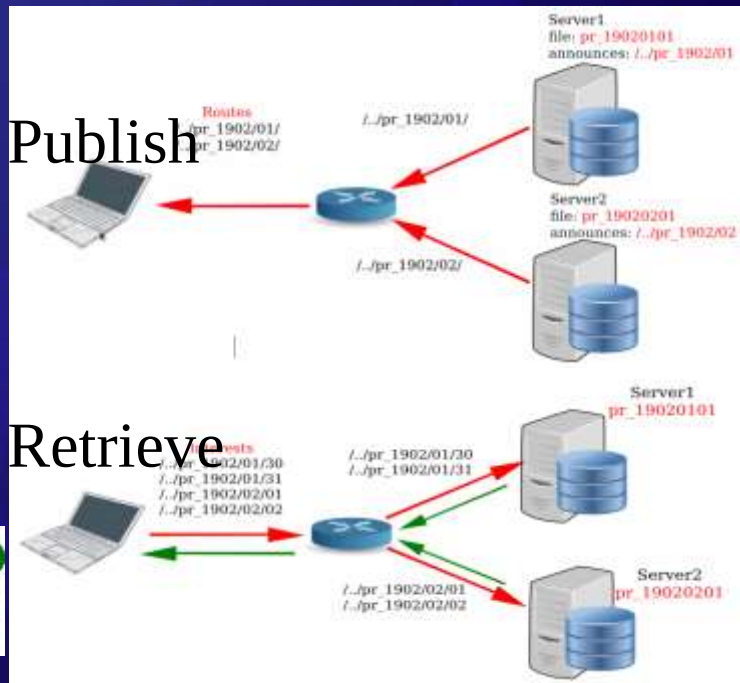
CC*IIE Campus Design: Northwest Indian College – Teaching/Learning & Science

- High speed connectivity for distance learning, including federated identity.
- Science DMZ to share GIS data, specimen catalogs, and experimental measurements
- Broader Impact: Give American Indian students broader access to catalogs and computing resources at other institutions.

CC*IIE Integration: Colorado State U Supporting Climate Applications over NDN

- **Need**: climate and other big data applications have overwhelmed existing networking and data management solutions
  - Data size and diversity
  - Naming, discovery, retrieval, sharing, etc.
- **Approach**: migrate workflows to NDN
  - Name based rather than host based paradigm
  - Easy migration: automatically translate existing ad-hoc names to structured NDN names
  - Evaluate over state-of-the-art NDN testbed deployed in partnership with ESnet
- **Benefit**: vastly simplified application and networking environment
  - Robustness and speed: in-network caching, efficient content distribution, automatic failover, security, etc.
  - Simplified management: highly structured, standardized naming across application domains
  - Trivial publishing, grouping and discovery





#1341099: NSF CC-NIE Integration award

Cybersecurity Innovation for Cyberinfrastructure (CICI)

- $11M
- Focus areas:
  - Data Provenance
  - Secure Architecture/Design
  - Cybersecurity Center of Excellence
  - Themes: Data Integrity, Secure Software Defined Networking (SDN), Identity Management, Secure Data Transfer, Secure Cloud
- Proofs of Concept/Operational Deployments encouraged

Secure and Trustworthy Cyberspace (SaTC)

- **$75M Annual Budget.**
- Supports fundamental scientific advances and technologies to protect cyber-systems from malicious behavior, while preserving privacy and promoting usability.
- Develop the foundations for engineering systems inherently resistant to malicious cyber disruption
- Cybersecurity is a *multi-dimensional problem*, involving both the strength of security technologies and variability of human behavior.
- Encourage and incentivize socially responsible and safe behavior by individuals and organizations
- Focus on Privacy: Dear Colleague Letter for new collaborations between Computer and Social Scientists, including a focus on privacy.

SaTC: Program Scope and Principles

Cast a wide net and let the best ideas surface, rather than pursuing a prescriptive research agenda

Engage the research community in developing new fundamental ideas and concepts

Promote a healthy connection between academia and a broad spectrum of pubic and private stakeholders to enable transition of innovative and transformative results

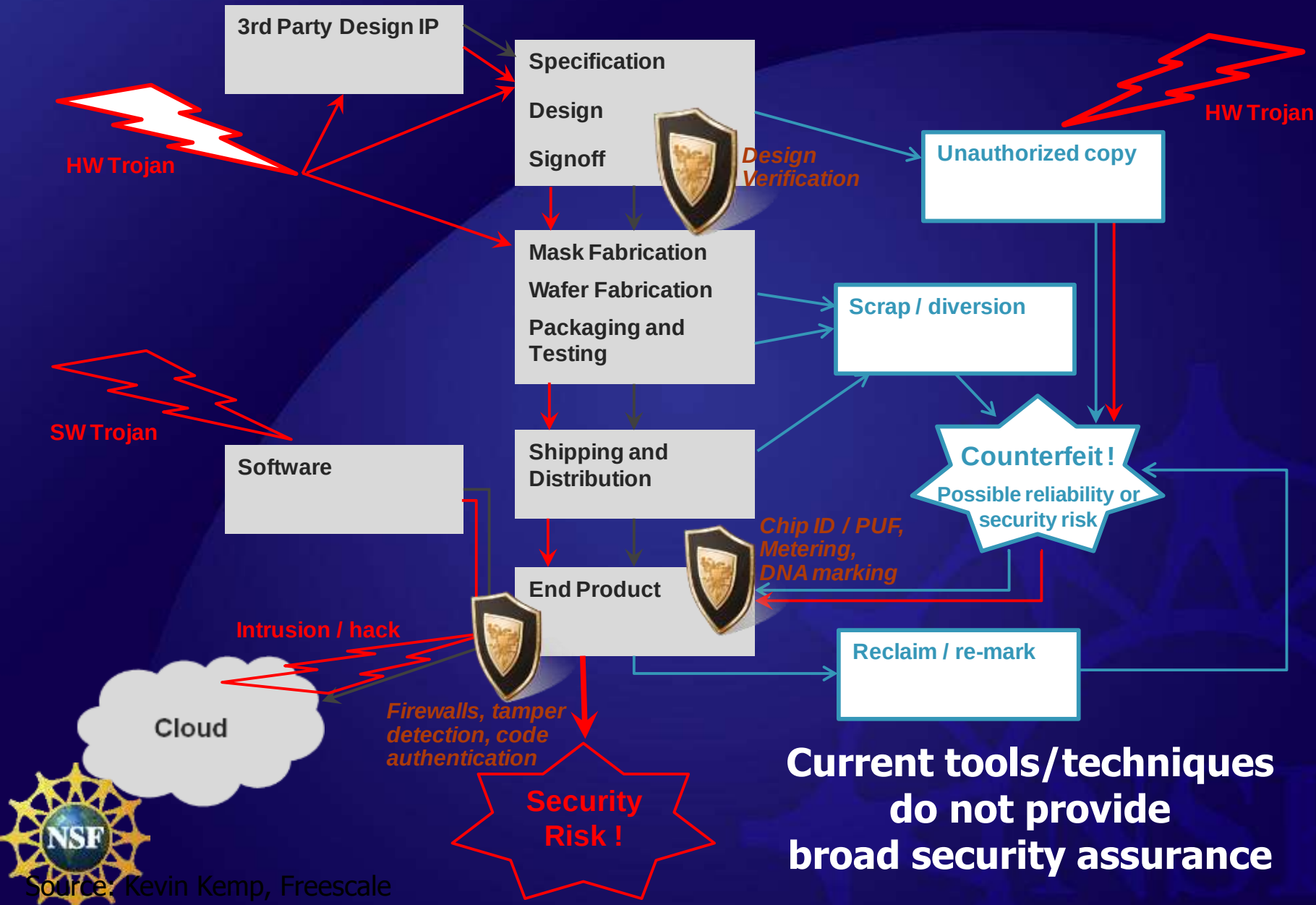
SaTC FY14 Funding Areas

Access control
Anti-malware
Anticensorship
Applied cryptography
Authentication
Cellphone network security
Citizen science
Cloud security
Cognitive psychology
Competitions
Cryptographic theory
Cyber physical systems
Cybereconomics
Cyberwar
Digital currencies
Education
Forensics
Formal methods
Governance
Hardware security
Healthcare security
Insider threat
Intrusion detection
Mobile security
Network security
Operating systems
Personalization
Privacy
Provenance
Security usability
Situational awareness
Smart Grid
Social networks
Sociology of security
Software security
Vehicle security
Verifiable computation
Voting systems security
Web security

Secure, Trustworthy, Assurted and Resilient Semiconductors and Systems (STARSS)

- Hardware security, with focus on *Design for Assurance*
- Jointly funded partnership between NSF and the Semiconductor Research Corporation (SRC)
- Partnership with SRC provides researchers greater insight and access to industry needs/capabilities/resources; facilitates transition to practice; and provides students opportunities to engage with industry.
- Supporting fundamental research to make semiconductors and systems more trustworthy and secure

Semiconductor Design & Manufacture Flow: Potential Points of Vulnerability to Attack/Theft



Current tools/techniques do not provide broad security assurance

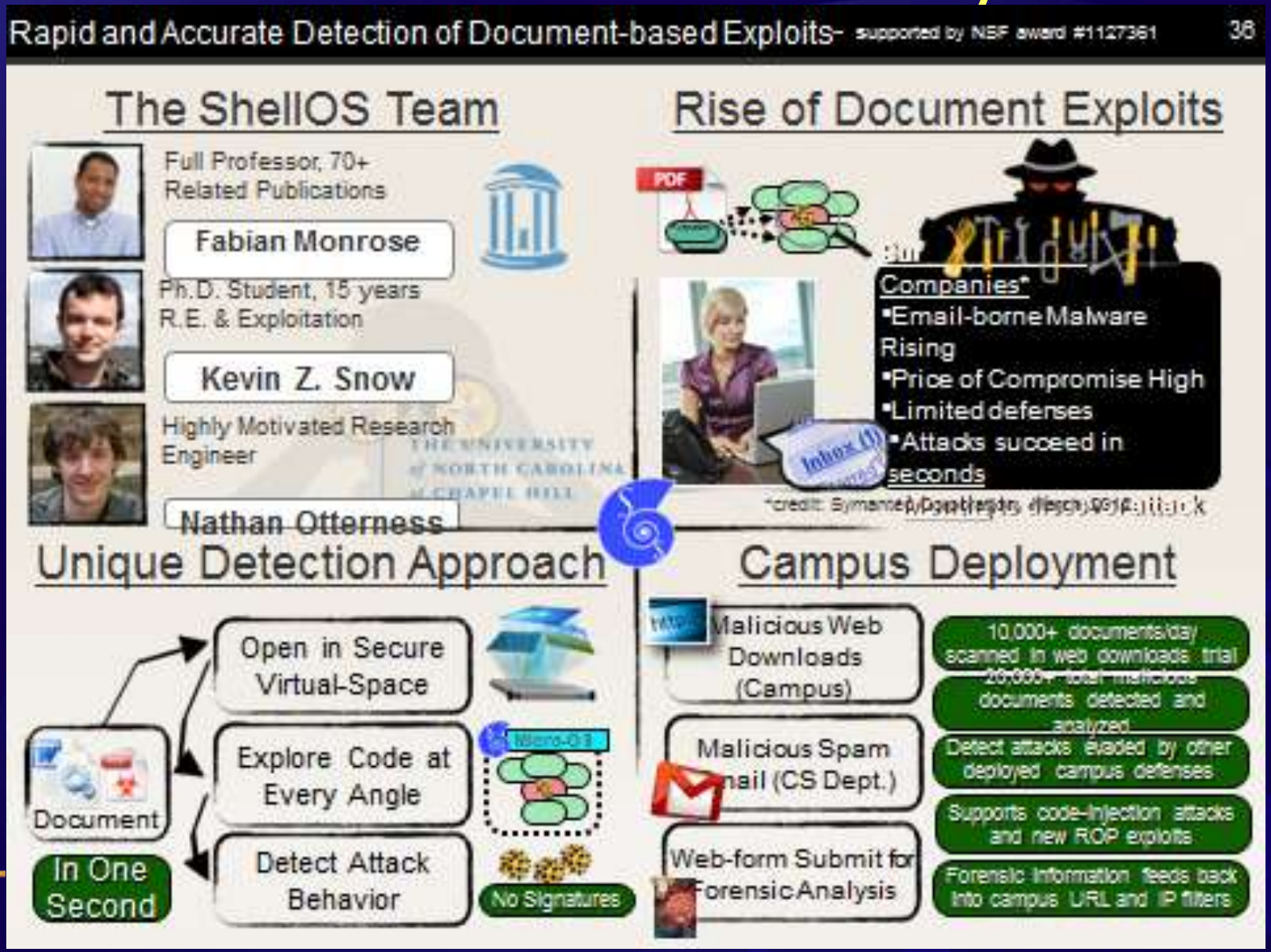
Source: Kevin Kemp, Freescale

SaTC: Social Behavioral and Economics (SBE) Example

Securing Cyber Space: Understanding the Cyber Attackers and Attacks via Social Media Analytics - Hsinchun Chen – U of Arizona

- **Objectives:**
  - Develop a computational social media analytics framework for text analytics and visualization of multilingual cybercriminal communities
  - Analyze cyberattacker motives, emerging threats and trends, cyberattacker community social structure, and hacker culture and market in the international hacker ecosystem
- **Methods:** Multiple data source from Cyberattacker community data (e.g. hacker forums, IRC channels, honeypots) in the United States, China, Russia, and the Middle-East
- **Prospective Broader Impact:** Development of automated multilingual content analysis methods, cyberattacker social media analytics techniques, and open source tools to support security researchers and social scientists

Transition to Practice: ShellOS Secure Document Analysis



Transition to Practice: Bro Network Security Monitor

- Bro provides a flexible, open network monitoring platform.
  - Developed since 1995, now at ICSI & NCSA.
  - Open-source with a BSD license.
  - Fundamentally different from a traditional IDS.

- Particularly well-suited for scientific environments.
  - Comprehensive logging for forensics.
  - Extensive standard library for typical, complex detection tasks.
  - Domain-specific scripting language for custom analysis.

- Bridges gap between academia and operations.
  - Has helped transition research into practice for almost two decades.
  - Deployed operationally by universities, research labs, Fortune 20.

- *Bro Center of Expertise* supports NSF community.
  - Provide assistance for operating and customizing Bro installations.
  - Develop new functionality tailored to the NSF community.
  - Support research community in transitioning technology into practice.

Sample of Small projects

- BGPSecurity/RPKI: "Exploring RPKI as a Solution for Secure Internet Routing"
- SDN Security: "Secure and Effective Policy Enforcement in Software Defined WANs"

Cybersecurity Education Funding Opportunities: CyberCorps®: Scholarship For Service (SFS)

- CyberCorps Scholarship for Service (**SFS**)
  - Increase the capacity of the United States higher education enterprise to produce professionals in these fields. Funding supports curriculum, outreach, faculty (Capacity BuildingTrack; $300-900 per project)
  - Increase the number of qualified students entering information assurance and computer security by providing funding to colleges and universities (Scholarship Track; $1-5M per project)
- Provides:
  - Tuition, fees, and stipends ($20-30K per year) for 2-3 final years of study (U.S. Citizens only).
  - Over 2000 scholarships have been awarded since the inception of the program. 51 participating universities with 475 students in school.
- About 75% at the master's level and 20% undergraduates.
- Over 93% of graduates go to work for the Government.
- Website: www.sfs.opm.gov

Research to Enable Smart Systems

Image Credit: *MicroStrain, Inc.*

Cyber-Physical Systems (CPS)

- ***Deeply integrate computation, communication, and control into physical systems***
- Aspects of CPS include pervasive computation, sensing and control; networking at multi- and extreme scales; dynamically reorganizing/reconfiguring systems; and high degrees of automation
- Dependable operation with high assurance of reliability, safety, security, and usability

Image Credit: *Bristol Robotics Lab*

National Robotics Initiative (NRI)

- ***Develop the next generation of collaborative robots, or co-robots, that work beside and cooperatively with people***
- A nationally concerted cross-agency effort among NSF, NASA, USDA, and NIH
- Initiative includes aim to understand the long-term social, behavioral, and economic implications
- Potential to enhance personal safety, health, and productivity

Application sectors

Transportation

Energy and Industrial Automation

Health and Medical Care

Critical Infrastructure

CyberPhysical Systems (CPS) Security

- Cross-cutting program that seeks fundamental scientific and engineering principles and technologies to underpin the integration of cyber and physical elements across all sectors: "systems you can bet your life on."
- Multi-agency solicitation including DHS Cyber Security Division, Department of Transportation and Federal Highway Administration, NIH
- Addresses Cybersecurity aspect of systems such as industrial controls
- NSF/Intel Partnership on Cyber-Physical Systems Security and Privacy

Questions?

Email me:
anikolic@nsf.gov