Image Credit: *Exploratorium*

Secure Smart Systems: A Global Imperative

Farnam Jahanian
CISE Directorate
National Science Foundation

NIST Cybersecurity for Cyber-Physical Systems Workshop
April 23, 2012

Smart Infrastructure

Imagine a day where…

static infrastructure is adaptable and safe

Image Credit: *MicroStrain, Inc.*

Environment and Sustainability

Imagine a day where…

we can forecast and mitigate ecological change

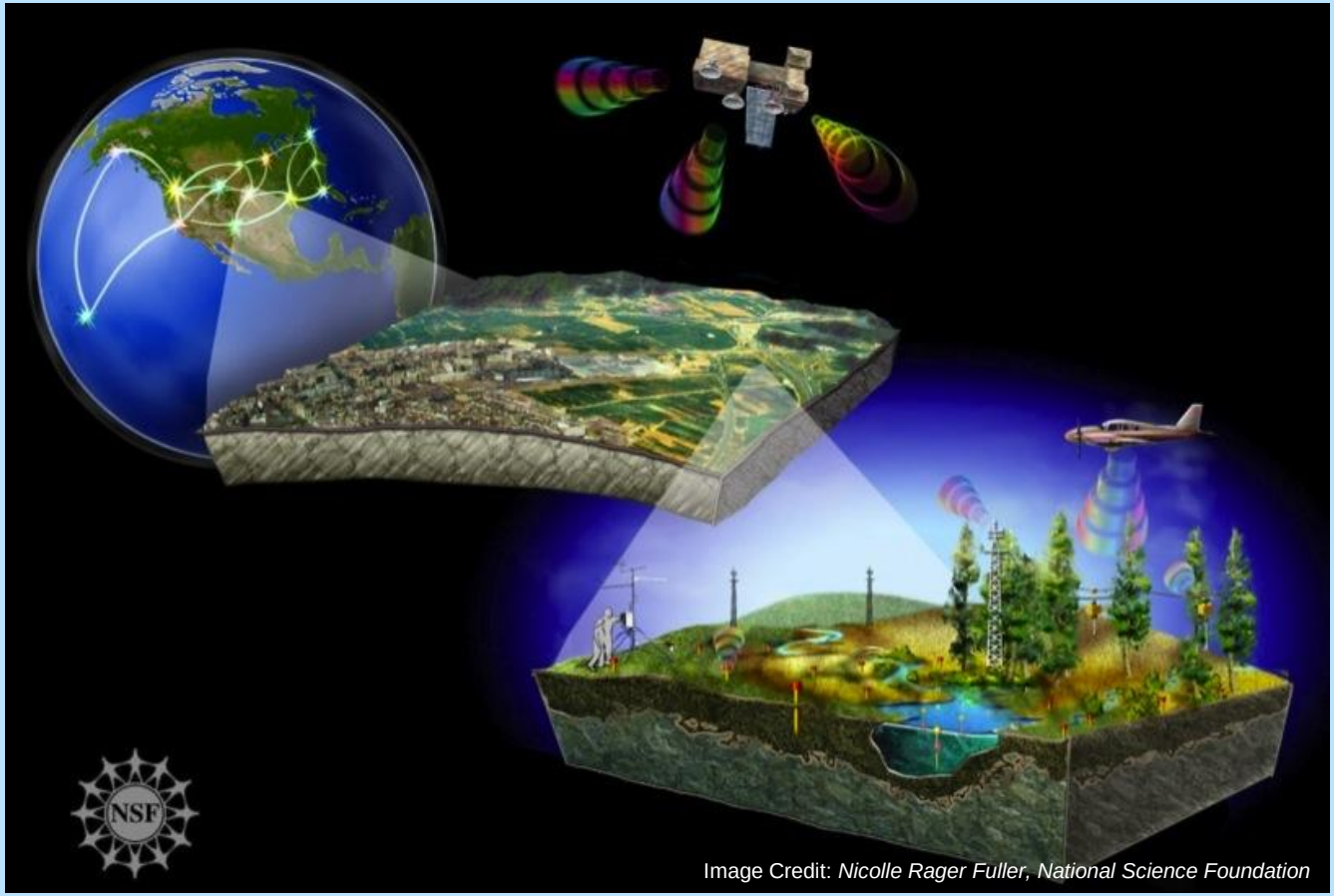
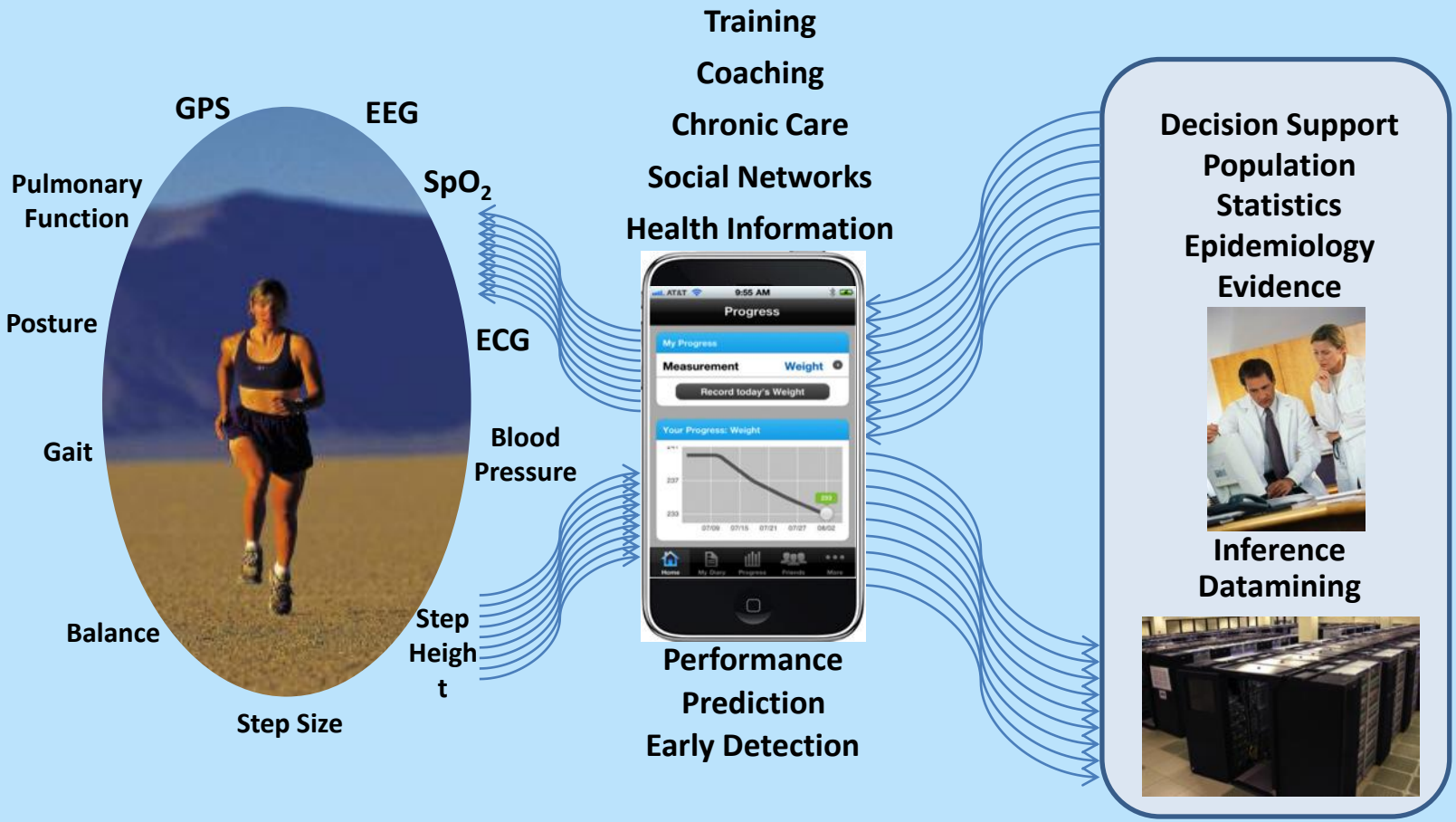


Image Credit: *Nicolle Rager Fuller, National Science Foundation*

Health and Wellbeing

Imagine a day where…

wellbeing is pervasive and healthcare is personalized



Smart Grids

Imagine a day where…

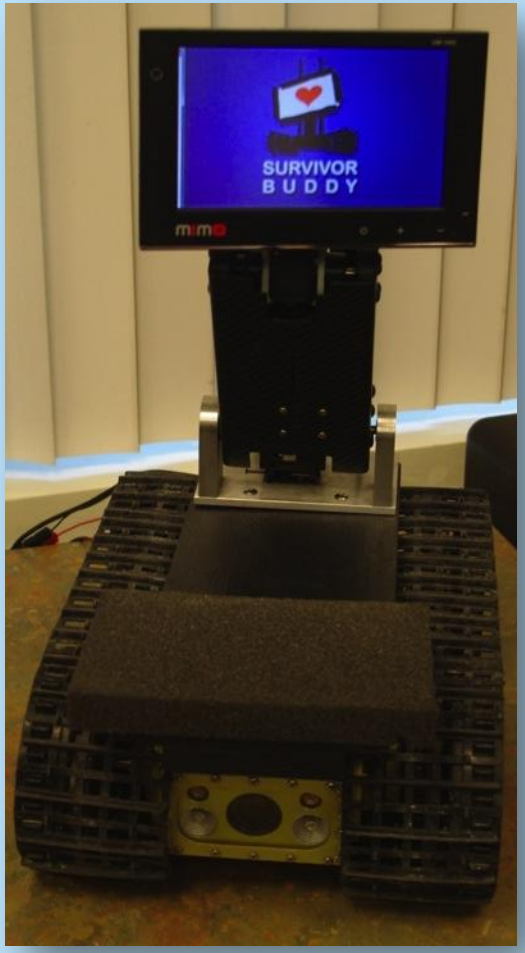
energy is efficiently used and intelligently managed

Image Credit: *Cisco, Inc.*

Emergency Response

Imagine a day where…

we can prevent, mitigate, and recover from disasters



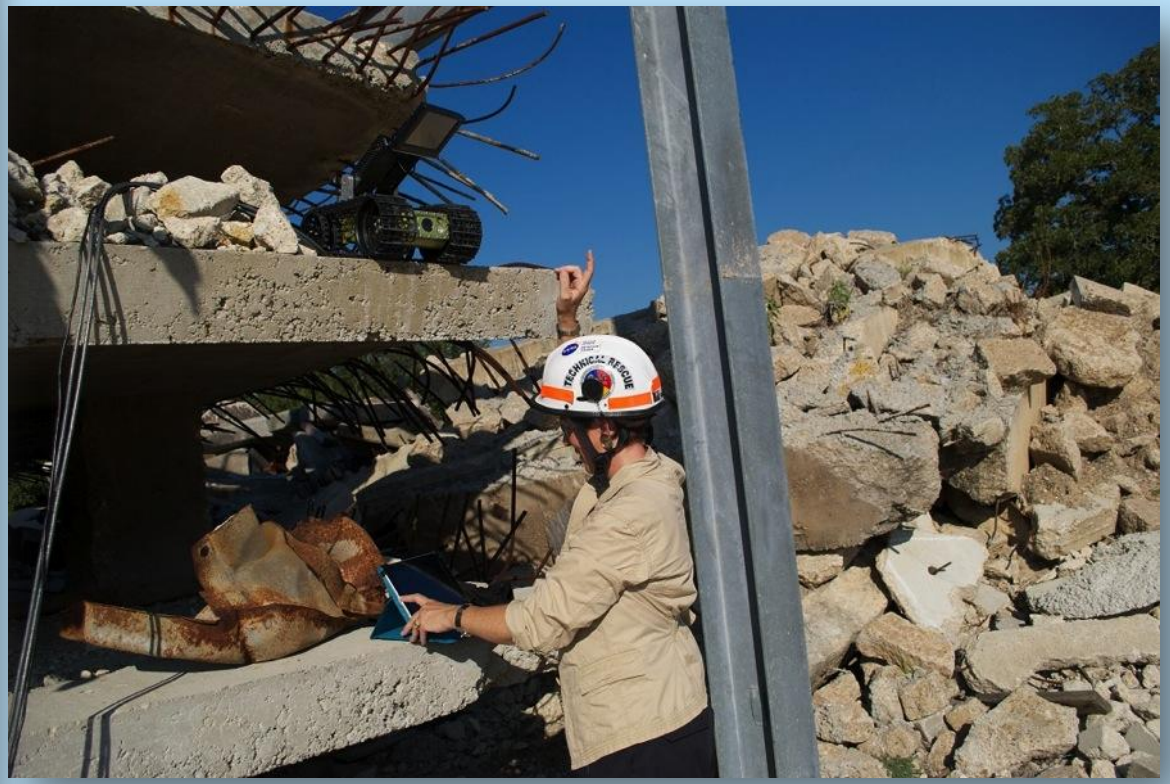


Image Credits: *Karen Geary, NSF* (left) and *Texas A&M University* (right)

Transportation: Safety and Energy

Imagine a day where…

traffic fatalities no longer exist

Image Credit: *PaulStamatiou.com*

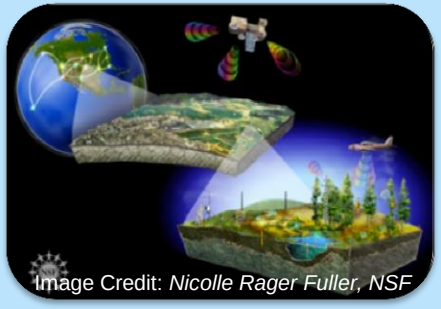
The Promise

Advances in *cyber-physical systems* hold the potential to reshape our world with more responsive, secure, and efficient systems that:

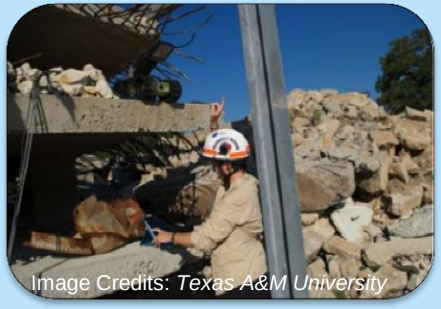
- transform the way we live
- drive economic prosperity
- underpin national security
- enhance societal well-being

CPS and National Priorities

Manufacturing, Robotics, & Smart Systems



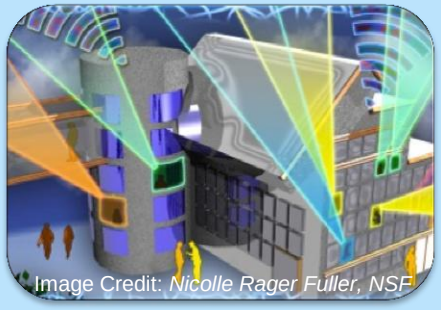
Environment & Sustainability



Emergency Response & Disaster Resiliency

Health & Wellbeing

Transportation & Energy



Broadband & Universal Connectivity

Secure Cyberspace

Education and Workforce Development

A National Imperative

- **2007 PCAST NITRD Report** – Recommended cross-disciplinary programs to accelerate work in CPS by Federal R&D agencies
- **2010 PCAST NITRD Report** – Expanded this recommendation to energy, transportation, health care, and homeland security
- **2011 PCAST Advanced Manufacturing Report** – Recommended investments to strength US leadership in the areas of robotics, cyber-physical systems, and flexible manufacturing

Cyber-Physical Systems

Deeply integrating computation, communication, and control into physical systems

- Pervasive computation, sensing and control
- Networked at multi- and extreme scales
- Dynamically reorganizing/reconfiguring
- High degrees of automation
- Dependable operation with high assurance of reliability, safety, security and usability

Transportation

- Faster and safer aircraft
- Improved use of airspace
- Safer, more efficient cars

Energy and Industrial Automation

- Homes and offices that are more energy efficient and cheaper to operate
- Distributed micro-generation for the grid

Healthcare and Biomedical

- Increased use of effective in-home care
- More capable devices for diagnosis
- New internal and external prosthetics

Critical Infrastructure

- More reliable power grid
- Highways that allow denser traffic with increased safety

Smart Systems: Sensing, Reasoning, and Decision

Environment Sensing







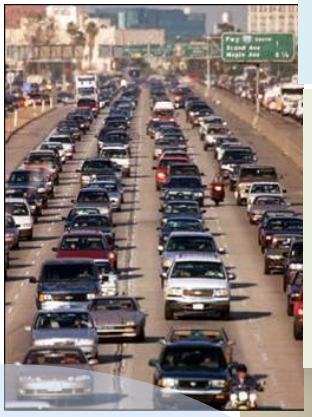
Percepts (sensors)

Agent (Reasoning)

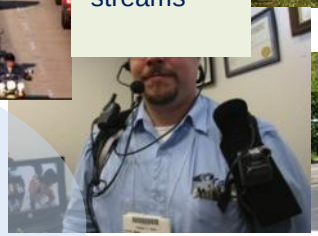
Actions (controllers)

Pervasive Computing

Emergency Response



Situation Awareness: Humans as sensors feed multi-modal data streams


People-Centric Sensing

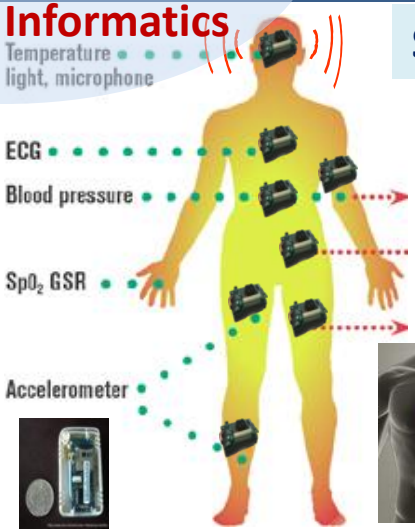
Social

Public Sensing

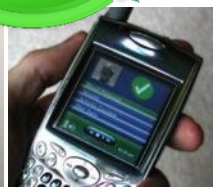
Personal Sensing

Social Sensing

Informatics



Smart Hearth Care

Source: Sajal Das, Keith Marzullo

Image Credit: Image courtesy of University of Florida

A Sea of Sensors

- We swim in **a sea of sensors and are drowning in data**:
  - Ability to analyze data in **real-time** and **retrospectively;** to create context for decisions; and to offer meaningful actionable feedback
  - As called for in the 2010 PCAST report, networked systems that not only **scale up**, but also **scale down** and **scale out**:
    - Smart, miniaturized, low-power, adaptive and self-calibrating instrumentation
    - Embedded sensors everywhere and connecting everything via networks leading to wide-scale sensing and control

- Research challenges:
  - Develop new scientific and engineering principles, algorithms, models, and theories for the analysis and design of CPS.
  - How do we build systems that combine the cyber and the physical world? Abstract representation of the physical world? Models for interaction w/ the physical world?

Realizing the Potential of CPS

- Establish a scientific basis for CPS: unified foundations, models, tools, and principles
- Synthesize knowledge from disciplines that interface the cyber and physical worlds to model and simulate complex systems and dynamics
- Enable usability, adoption, and deployment of complex systems through fundamental cognitive, behavioral, economic, social, and decision sciences
- Design for reliable, robust, safe, scalable, secure, and certifiably dependable control of complex systems – CPS people can bet their lives on
    - Support networked, cyber-physical systems with built-in assurance, safety, security, and predictable performance
- Develop, document, and disseminate research-based standards and best practices for CPS
- Advance cyber-enabled discovery and innovation to enhance understanding and management of complex systems
- Prepare the next generation of talent for CPS through education and workforce development

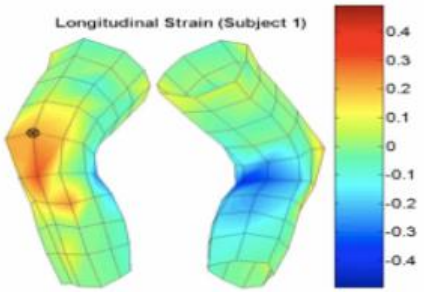
Enable a research community and workforce that will be prepared to address the challenges of next generation systems

Bridge previously separated areas of research to develop a unified systems science for cyber-physical systems

Develop new educational strategies for a 21st century CPS workforce that is conversant in both cyber and physical aspects of systems

NSF CPS Awards Span Many Sectors

Assistive Medical Technologies: Programmable second skin senses and re-educates injured nervous systems. (Eugene Goldfield, Harvard Medical School)



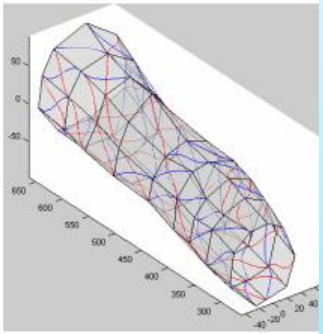


Image Credit: *Wyss Institute, Harvard University*

Environmental Sensing: Modeling and software allow actuated sensing in dynamic environments, such as rivers. (Jonathan Sprinkle, U. Arizona; Sonia Martinez, UCSD; Alex Bayen, UC Berkeley)

Autonomous Vehicles: Development of precision and real-time sensors, smart algorithms, and verification tools enables self-driving cars. (Ragunathan "Raj" Rajkumar, CMU, et al.)

How can we design, build and verify reliable, predictable, safe and **secure** cyber-physical systems upon which people can - and will - bet their lives?

Image Credit: *CCC and SIGACT CATCS*

A World of Cyber Threats

- DDoS attacks
- Worms
- Trojan Horses
- Spyware
- Botnets
- Phishing
- Insider misuse
- Data theft

Image Credit: *Nicolle Rager Fuller, NSF*

Why is the Cyber Security Challenge so Difficult?

- **Attacks and defenses co-evolve**: a system that was secure yesterday might no longer be secure tomorrow.
- The technology base of our systems is frequently updated to improve functionality, availability, and/or performance. **New systems introduce new vulnerabilities** that need new defenses.
- The **environments** in which our computing systems are deployed and the functionality they provide are **dynamic**, e.g. cloud computing, mobile platforms.
- The **sophistication** of attackers is increasing as well as their sheer **number** and the **specificity** of their targets.
- As **automation pervades new platforms**, vulnerabilities will be found in critical infrastructure, automotive systems, medical devices.
- Cyber security is a **multi-dimensional** problem requiring expertise from CS, mathematics, economics, behavioral and social sciences.

The Early Years: *'Cyber Vandalism'*

- Primary motivation of hackers was bragging rights
- Worms and viruses intended to simply wreak havoc on the infrastructure
- These were availability attacks: impacting network access and services, and often, reputations

The Rise of Botnets: Cyber Crime

- Dramatic Transformation and Escalation
  - A compromised system is more useful alive than dead
  - A compromised system provides anonymity
  - A network of compromised hosts provides a powerful delivery platform
- Botnets represent today's attack platform
- Botnets will continue to dominate how attacks are launched

Rank	Family	Primary Control Mechanism	Computers Cleaned (1Q10)	Computers Cleaned (2Q10)	Change
1	Win32/Rimecud	Other	1,807,773	1,748,260	-3.3% ▼
2	Win32/Alureon	HTTP	1,463,885	1,035,079	-29.3% ▼
3	Win32/Hamweq	IRC	1,117,380	779,731	-30.2% ▼
4	Win32/Pushbot	IRC	474,761	589,248	24.1% ▲
5	Win32/IRCbot	IRC	597,654	388,749	-35.0% ▼

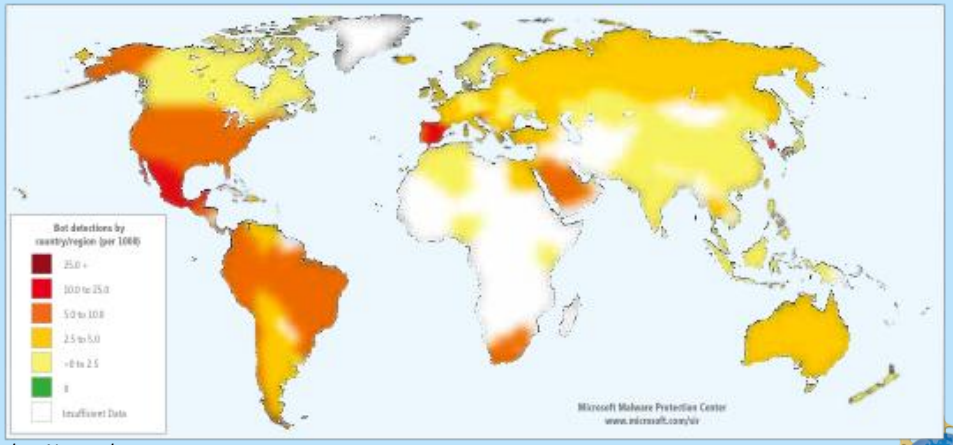


Image Credit: *Arbor Networks*

Microsoft desktop anti-malware products removed bots from 6.5 million computers around the world in 2Q10 [Microsoft SIR v9]

Cheaper, Better, Faster

- While Internet threat complexity is increasing at a dramatic rate, costs are dropping

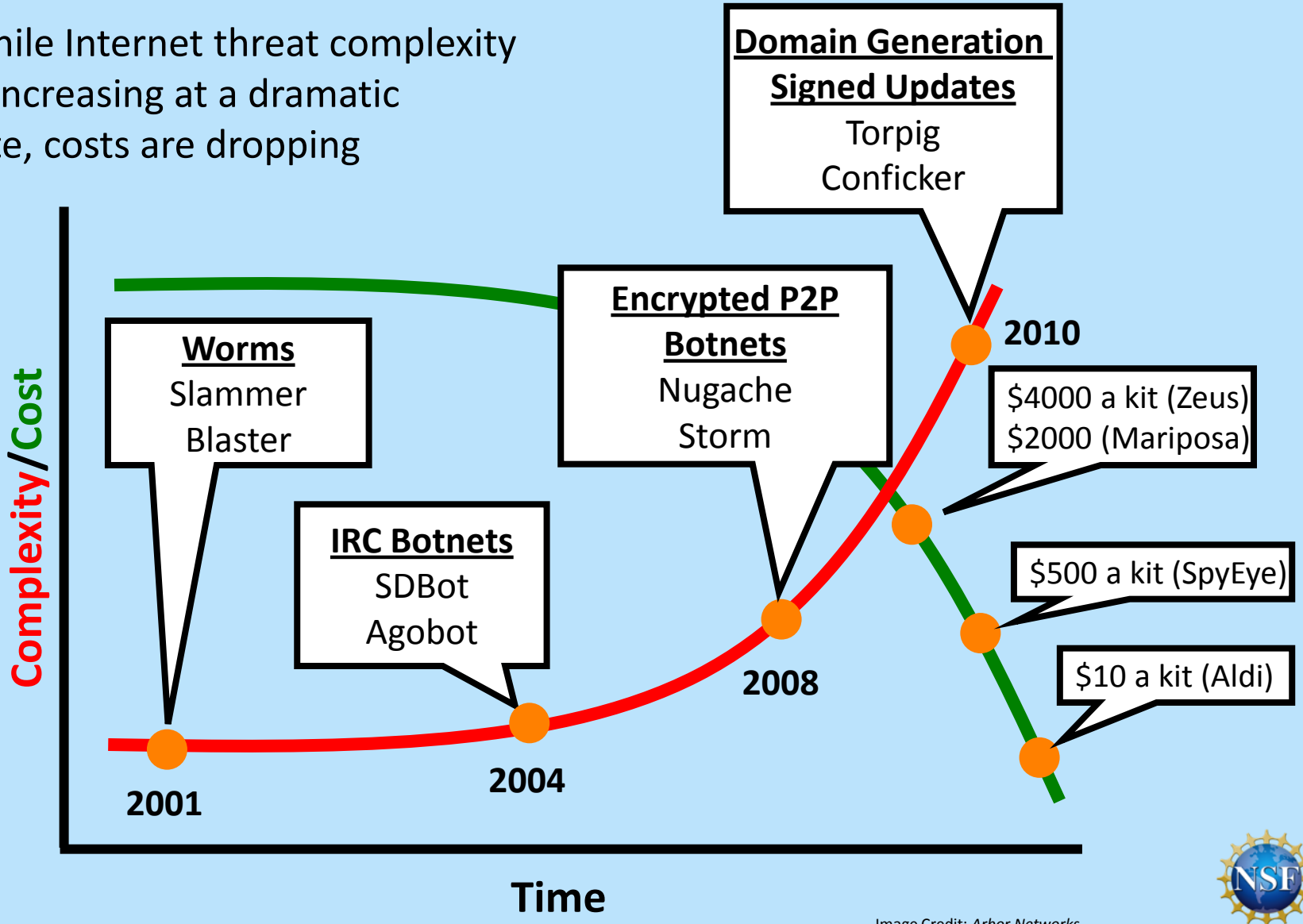
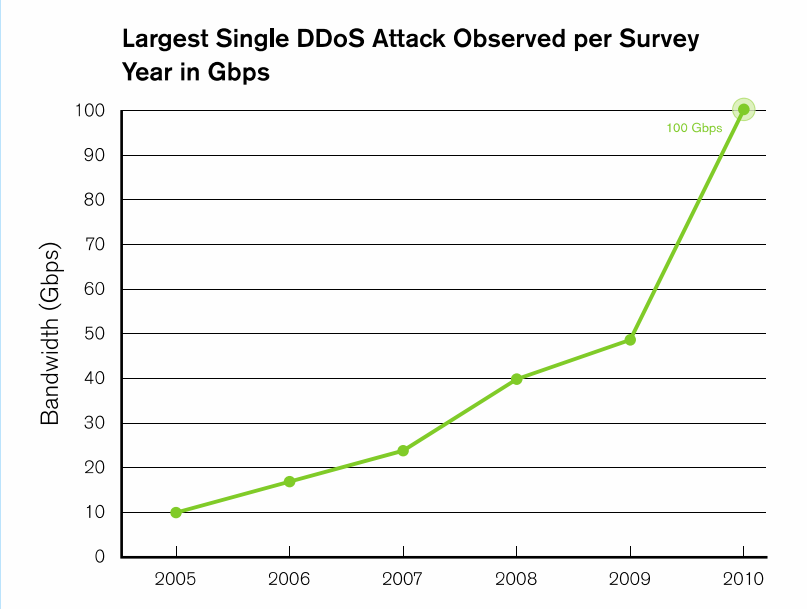


Image Credit: *Arbor Networks*

Increasing Size, Sophistication, Targeting



- Increasing size and sophistication
- 10-100Gbps DDoS attacks seen by ISPs
- Attacks moving "up" – Attacking services rather than infrastructure

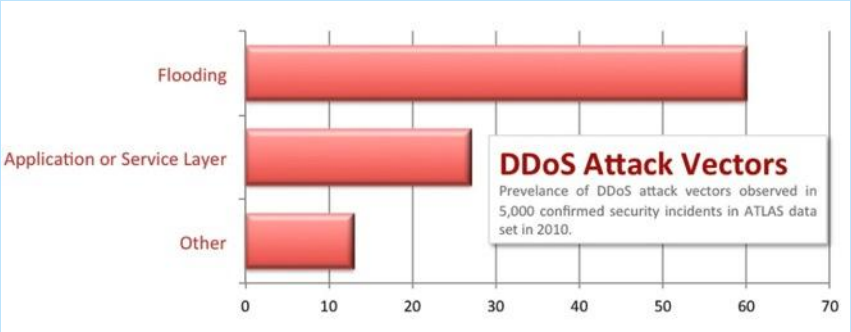
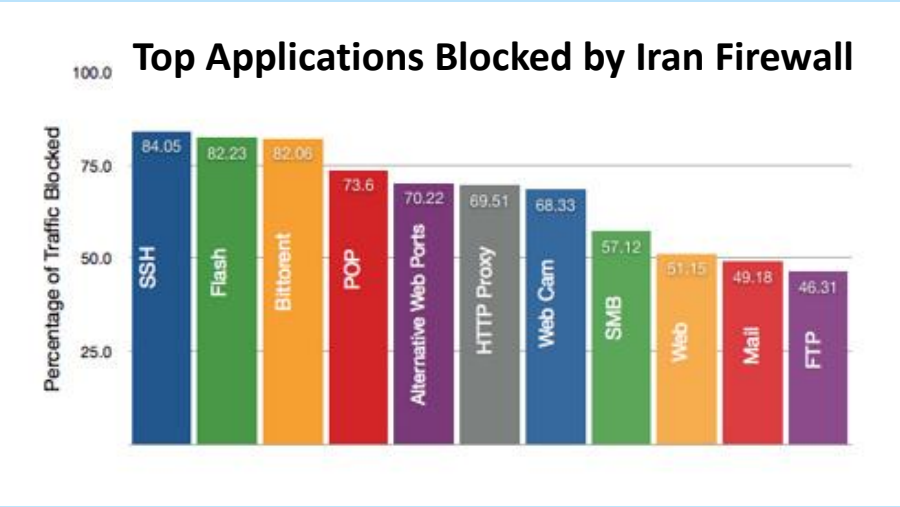
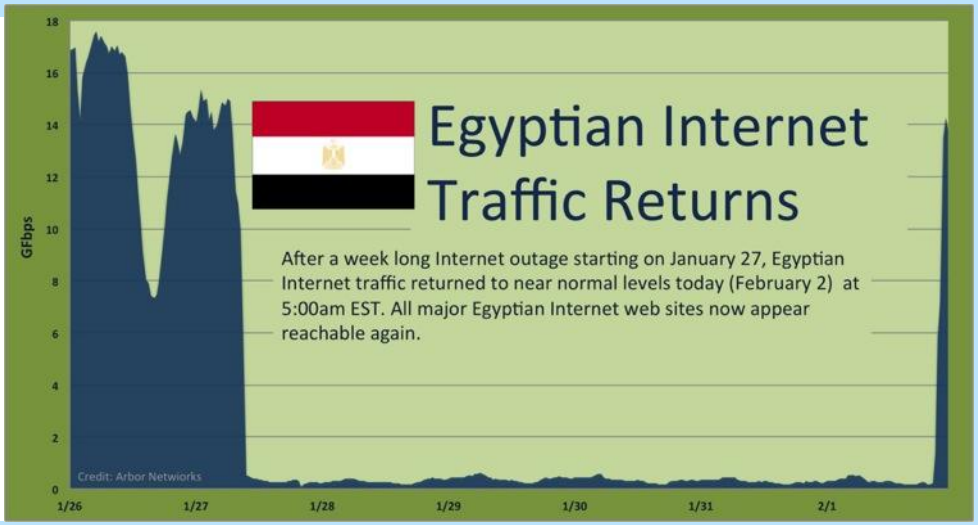


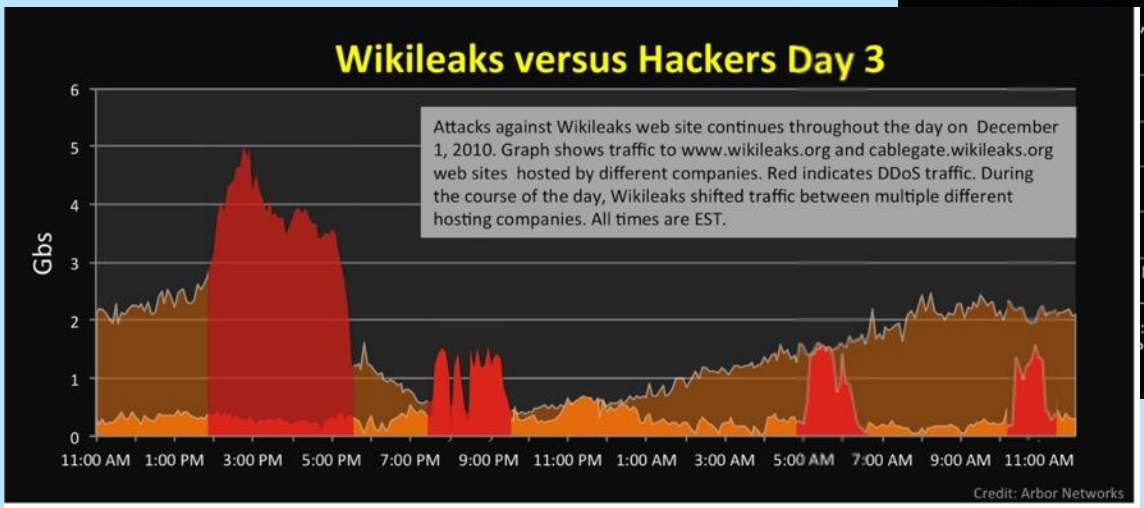
Image credits: *Arbor Networks*

- Exploits moving "up" as well – infections now delivered via web sites through drive-by installs
  - Projected 1 in 10 web sites hosts malicious content
  - Web-based delivery means outpacing email, viruses, etc.

Cyber-war, Censorship, Activism, and the Rise of Politically Motivated Attacks







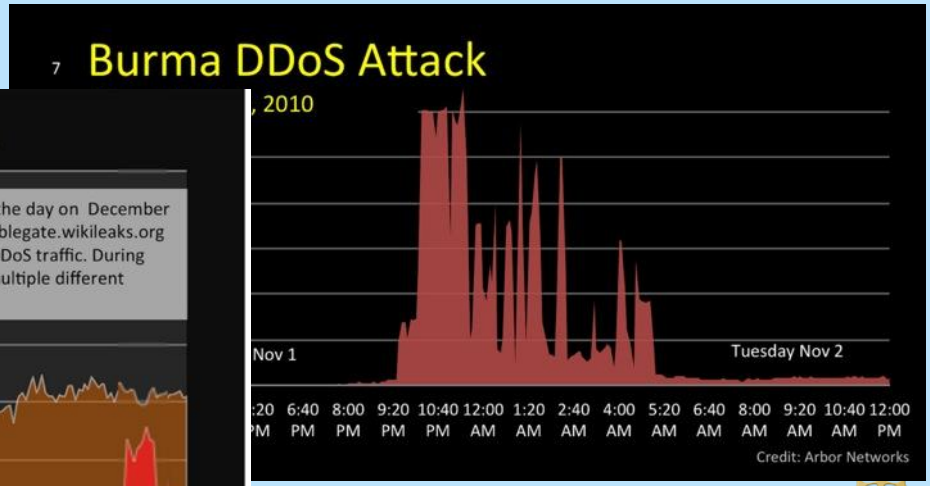


Image credits: *Arbor Networks*

Evolution of Cyber Threats

Future security challenges will follow technology & Internet adoption patterns:

Image Credit: *Nicolle Rager Fuller, National Science Foundation*

- Botnets will continue to dominate how attacks are launched; attribution and forensics is increasingly difficult.
- Distributed attacks increasing in size and sophistication, targeting specific applications.
- Proliferation of attacks spurred by financial gains and now political motives.
- Proliferation of wireless devices and social media platforms open new avenues for hackers.
- Protecting cloud infrastructure key to long-term adoption.
- The trend toward increasingly cyber-enabled systems expands the scope of attacks to physical infrastructure – manufacturing, energy production, healthcare and transportation.

As the trend towards increasingly cyber-enabled systems grows, so does the need to secure those systems.

Cyber-Physical Security Risks

Image Credit: *Matt Blaze*

Law Enforcement Communications

Image Credit: *Karl Koshner*

Automobiles

Embedded Medical Devices

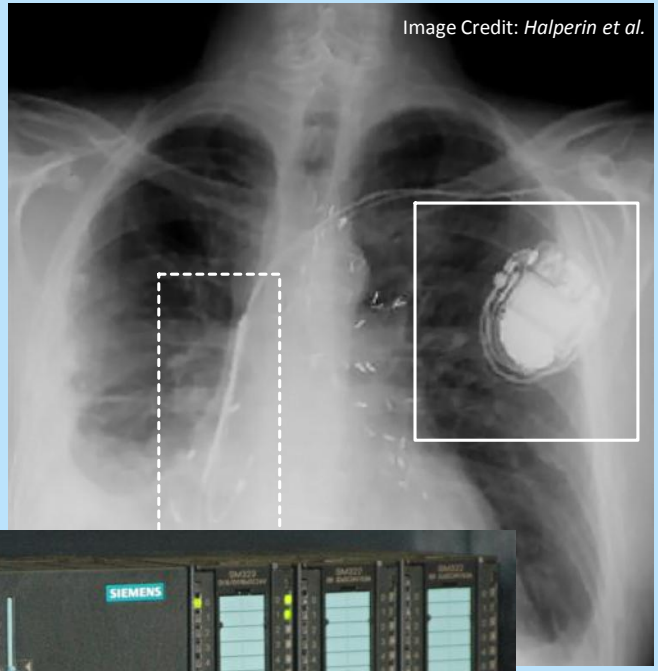


Image Credit: *Halperin et al.*

Control Systems

Security Risks in Automotive Computers and Networks

- Computer scientists and engineers have demonstrated ability to remotely take over automotive control systems
- In one case, by connecting to a standard diagnostic computer port included in late-model cars, caused disruption to brakes, speedometer reading, and vehicle telematics
- They are now working with the automotive industry to develop new methods for assuring the security as well as safety of automotive electronics

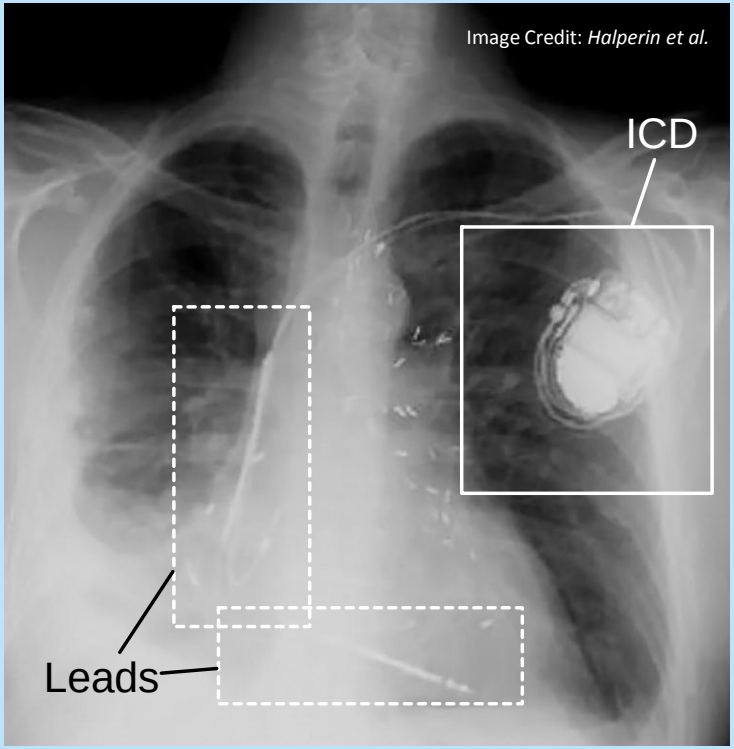
Image Credit: *Karl Koshner*

This car was not moving

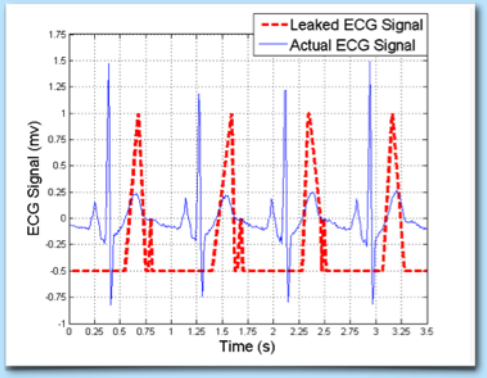
Stefan Savage (UC San Diego) and Tadayoshi Kohno (U Washington)

Medical Device Security

As of 2006, more than half of medical devices on the US market now contain and trust software.

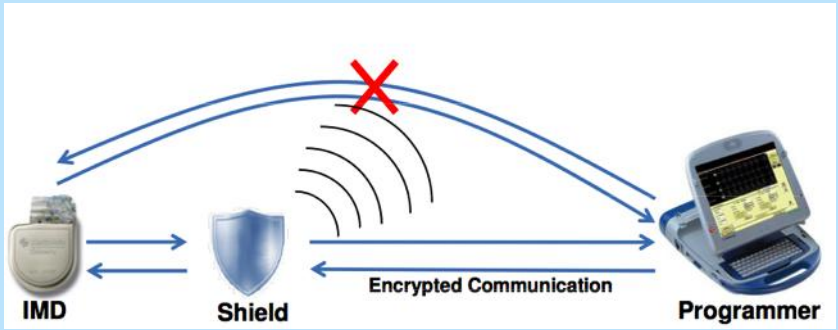


Defibrillator Vulnerabilities, Zero-Power Defenses
[Halperin et al., IEEE S&P '08]



Telemedicine Privacy
[Salajegheh et al., J. Med. Dev. '09]

AED Security
[Hanna et al., HealthSec '11]

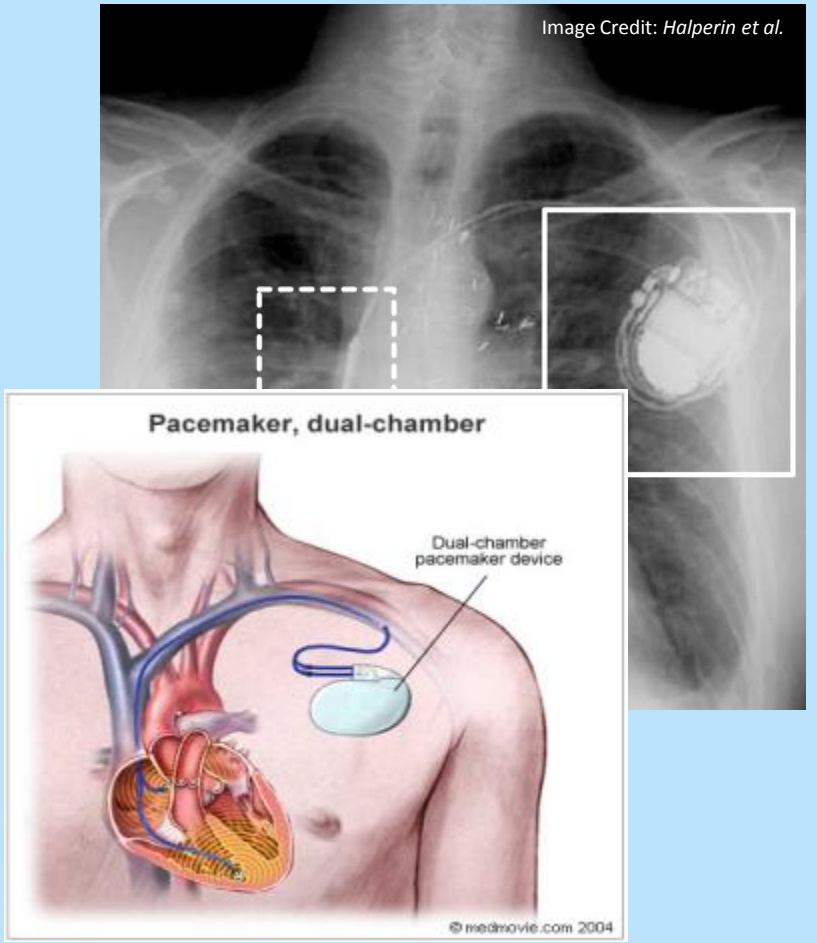


Radio Shield/Jamming for Implants
[Gollakota et al., ACM SIGCOMM '11]

Funded by NSF CNS-0435065, CNS-0520729, CNS-0627529, CNS-0831244, CNS-0842695

Implantable Medical Device Security

- Implanted medical devices frequently incorporate wireless control
- By gaining wireless access to a combination heart defibrillator and pacemaker, were able to reprogram it to shut down and to deliver jolts of electricity
- Attack vector: the device test mechanism, wireless communication interface with a control mechanism that was unencrypted
- Computer scientists working with physicians found new ways to secure these devices against extraneous signals and wireless attacks
- Encryption but also “cloakers” – make your implants “invisible” at your discretion



PI: Kevin Fu, UMass – Amherst

[Halperin et al., IEEE Symposium on Security & Privacy 2008]

How Much SW in Medical Devices?

- 1983-1997
  - 6% of all recalls attributed to SW
- 1999-2005
  - **Almost doubled**: 11.3% of all recalls attributed to SW
  - 49% of all recalled devices relied on software (up from 24%)
- 1991-2000
  - **Doubled**: # of pacemakers and ICDs recalled because of SW

- 2006
  - Milestone: Over half of medical devices now involve software
- 2002-2010
  - 537+ recalls of SW-based devices affecting 1,527,311+ devices

[Sources: Bliznakov et al. 2006, Faris 2006, Maisel et al. 2002, Wallace & Kuhn 2001, Computer history museum, eurogramer.net, wikipedia, businesspundit.com, imdb.com, coverbrowser.com, thefilmtalk.com]

SCADA Security

- Targets industrial control systems, such as power plants
- Enters an organization thru an infected removable drive
- Zero-day exploits
- Anti-virus evasion techniques
- P-2-P update propagation
- Reprogramming PLC code
- Sophisticated exploitation of attack surface for a CPS

Action Webs:
Networked embedded sensor-rich systems

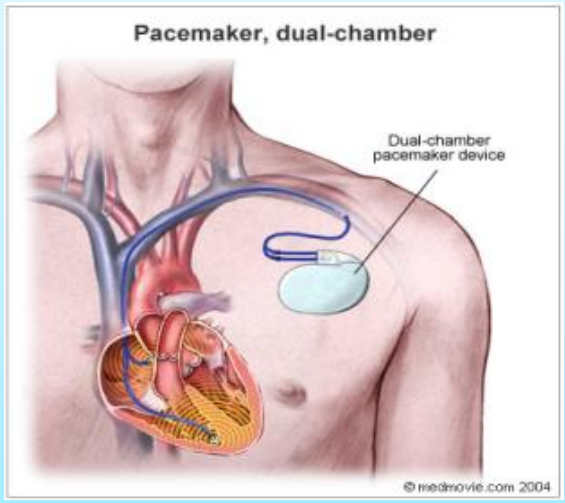
Image Credit: *Cisco, Inc.*

- Modeling, testing and validating “action webs” to achieve high-confidence networked sensor-rich control systems
- Approach: develop a theory of “action webs” using stochastic hybrid systems; taskable, multi-modal, and mobile sensor webs; and multi-scale action-perception hierarchies
  - With focus on cybersecurity: threat assessment, attack diagnosis, and resilient control
- Applications:
  - Intelligent Buildings for optimal heating, ventilation, air conditioning, and lighting based on occupant behavior and external environment
  - Air Traffic Control for mobile vehicle platforms with sensor suites for environmental sensing to enable safe, convenient, and energy efficient routing

Claire Tomlin (UC Berkeley), et al.

Design and Certification of Dependable Open Systems

- Certification and approval process are staggering
- Safety certification practice typically supports fixed configuration
- Wireless, open systems and interoperation introduce many new certification challenges



Improving Device Safety:
In cooperation with FDA, NSF projects are underway to design, validate, and accelerate certification of medical devices.
(University of Illinois, University of Pennsylvania, Harvard Medical/Mass General, University of Maryland, Kansas State University)

Insup Lee (U Penn), et al.

Foundations of Secure Cyber Physical Systems

- Cyber-physical systems regulating critical infrastructures, such as electrical grids and water networks, are increasingly geographically distributed, necessitating communication between remote sensors, actuators and controllers
- Combination of networked computational and physical subsystems leads to new security vulnerabilities that adversaries can exploit
- Approach: design new secure protocols and architectures for CPS through a unified conceptual framework - models for the physical system and the communication/computation network to define precise attack models and vulnerabilities
- Models are used to design protocols with provable security guarantees, thus enabling the design of more trustworthy architectures and components
- Applications: smart buildings, transportation networks, and smart grids

Image Credit: *Cisco, Inc.*

Suhas Diggavi (UCLA), et al.

Smart Grid Security

- ***The CyberPhysical Challenges of Transient Stability and Security in Power Grids***

  Ian Dobson (Iowa State University), et. al.

  – Focuses on the analysis of instabilities of electric power networks, and on design of cyber-physical control methods to monitor, detect, and mitigate them

  – The controls must perform robustly in the presence of variability and uncertainty in electric generation, loads, communications, and equipment status, and during abnormal states caused by natural faults or malicious attacks

- ***Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) at the Univ. of Illinois***

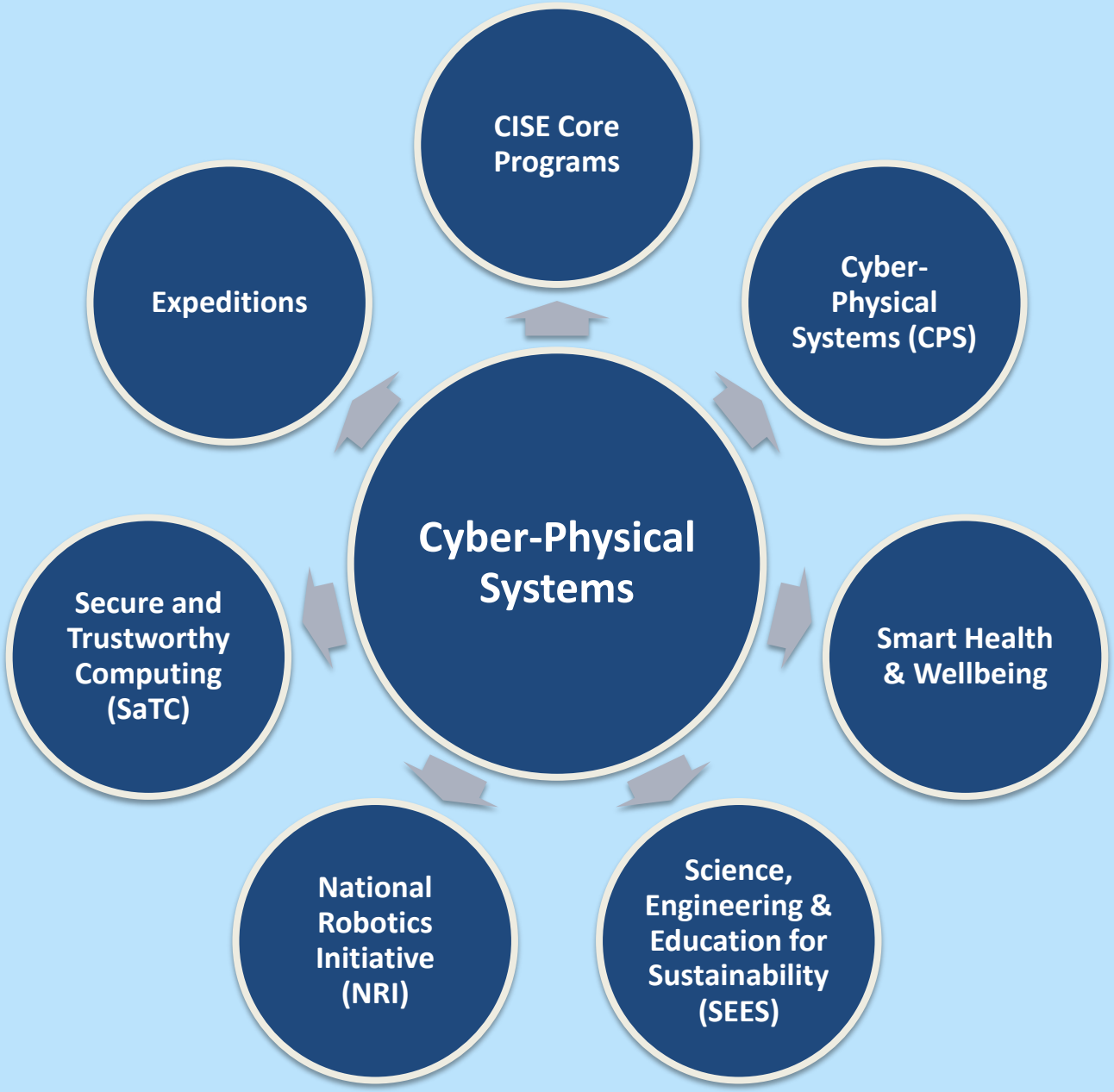
  – Focused on securing the low-level devices, communications, and data systems that make up the power grid, to ensure trustworthy operation during normal conditions, cyber-attacks, and/or power emergencies

- ***Information and Computation Hierarchy for Smart Grids*** - WenZhan Song (GSU), et. al.

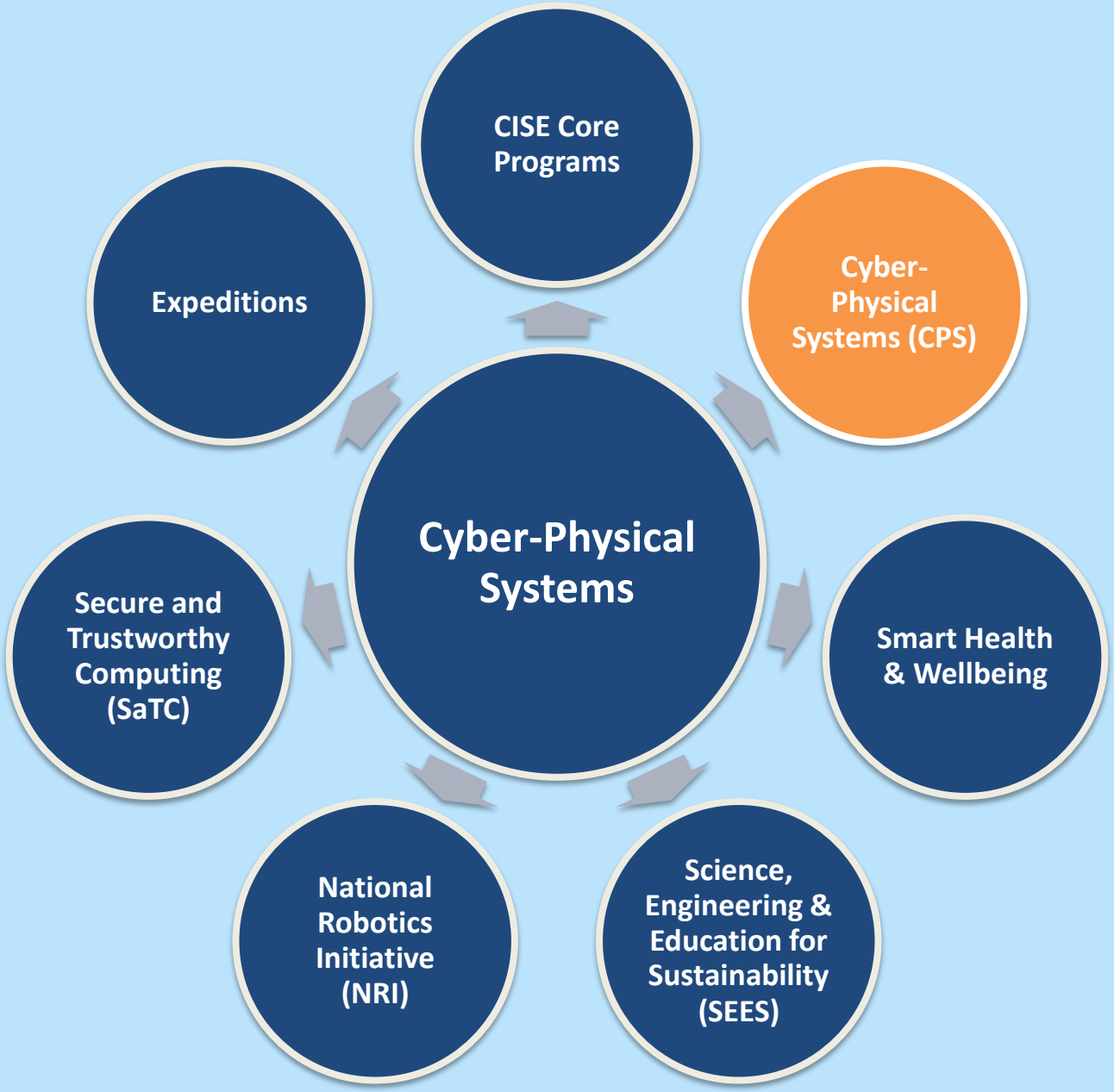
  – Support for high penetrations of renewable energy sources, community based micro-grids, and the widespread use of electric cars and smart appliances

  – Investigates cloud-based computing architecture for smart grids, and temporal and spatial characteristics of information hierarchy

CPS Support across NSF



CPS Support across NSF



Cyber-Physical Systems Program

Deeply integrating computation, communication, and control into physical systems

- Launched in 2009
- Aims to develop the core system science needed to engineer complex "smart" cyber-physical systems
- Serves key national priorities
- Coordinated across NSF and with other government agencies

Transportation

Manufacturing and Industrial Automation

Energy

Healthcare and Biomedical

Critical Infrastructure

114 active awards:

- $140M+ total investment
- 43 small, average $527K
- 66 medium, average $1.5M
- 5 large, average $4.7M

Cross-Directorate Solicitation: CISE and ENG

Three CPS Research Themes

- ***Science*** *of Cyber-Physical Systems:* New models and theories that unify perspectives, capable of expressing the interacting dynamics of the computational and physical components of a system in a dynamic environment. A unified science would support composition, bridge the computational versus physical notions of time and space, cope with uncertainty, and enable cyber-physical systems to interoperate and evolve.
- ***Technology*** *for Cyber-Physical Systems:* New design, analysis, and verification tools are needed that embody the scientific principles of CPS, and that incorporate measurement, dynamics, and control. New building blocks are also needed, including hardware computing platforms, operating systems, and middleware.
- ***Engineering*** *of Cyber-Physical Systems:* New opportunity to rethink principles of systems engineering, built on the foundation of CPS science and technology and able to support open cyber-physical systems. Focus on system architecture, design, integration, and design space exploration that produce certifiably dependable systems.

FY12 Solicitation

Breakthrough projects:

- Must offer a significant advance in fundamental CPS science, engineering and/or technology that has the potential to change the field
- Up to $750K for 3 yrs

Synergy projects:

- Must demonstrate innovation at the intersection of multiple disciplines, to accomplish a clear goal that requires an integrated perspective spanning the disciplines
- $750K to $2M for 3-4 yrs

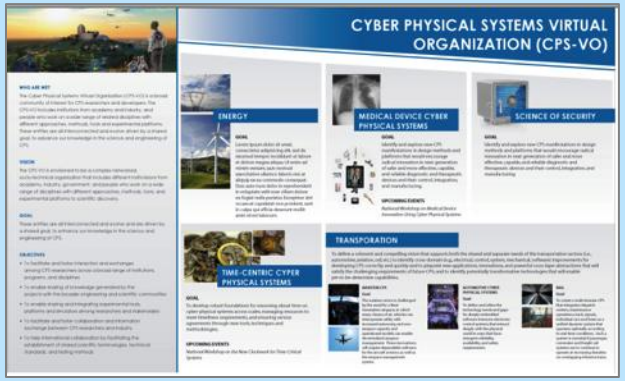
Frontiers projects:

- Must address clearly identified critical CPS challenges that cannot be achieved by a set of smaller projects
- $1.2M to $10M for 4-5 yrs

CPS Virtual Organization (VO)

Objectives:

- Community building
- Technical support for collaboration
- Technology transfer and translational research
- International collaboration



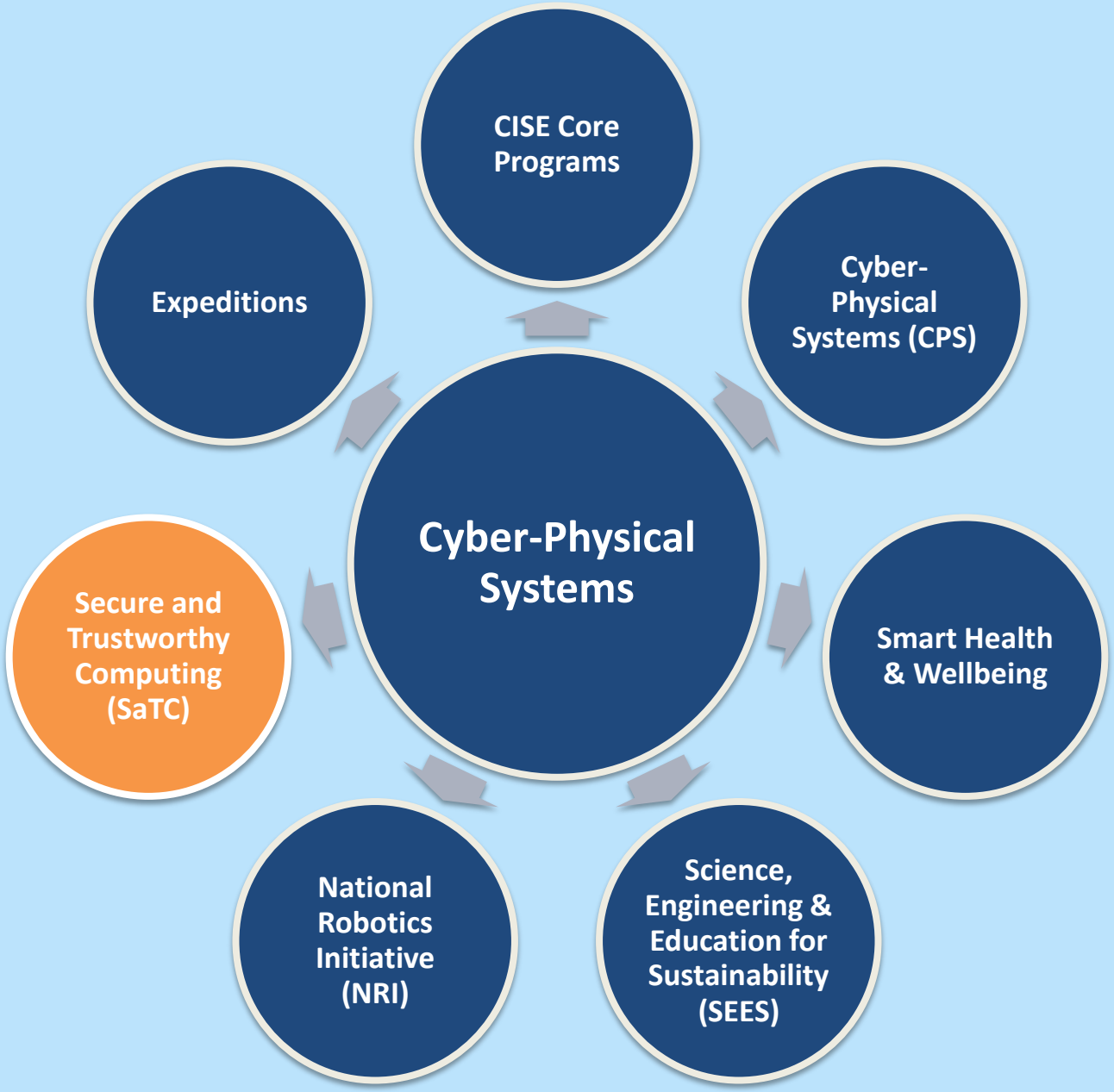
http://cps-vo.org

Principles & Services:

- Community controlled
  - Information dissemination to and by the research community
- Services for collaborative activities Support for SIGs
- Industry academy interactions
- Built on open source framework
- Home for the community's historical reference materials
- Advertising of new events (e.g., calendar of upcoming events)
- Discussion forums and instant messaging
- Community members list and matchmaking

~1000 users + increasing interest by other federal agencies to provide open source results and to increase interactions among research communities

CPS Support across NSF



Secure and Trustworthy Cyberspace (SaTC)

Securing our Nation's cyberspace

- Aims to support fundamental scientific advances and technologies to protect cyber-systems from malicious behavior, while preserving privacy and promoting usability.

- Program addresses three perspectives:
  - Trustworthy Computing Systems
  - Social, Behavioral and Economic Sciences
  - Transition to Practice

Image Credit: *ThinkStock*

Cross-Directorate Effort: CISE, ENG, EHR, MPS, OCI, and SBE

SaTC: Program Scope and Principles

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

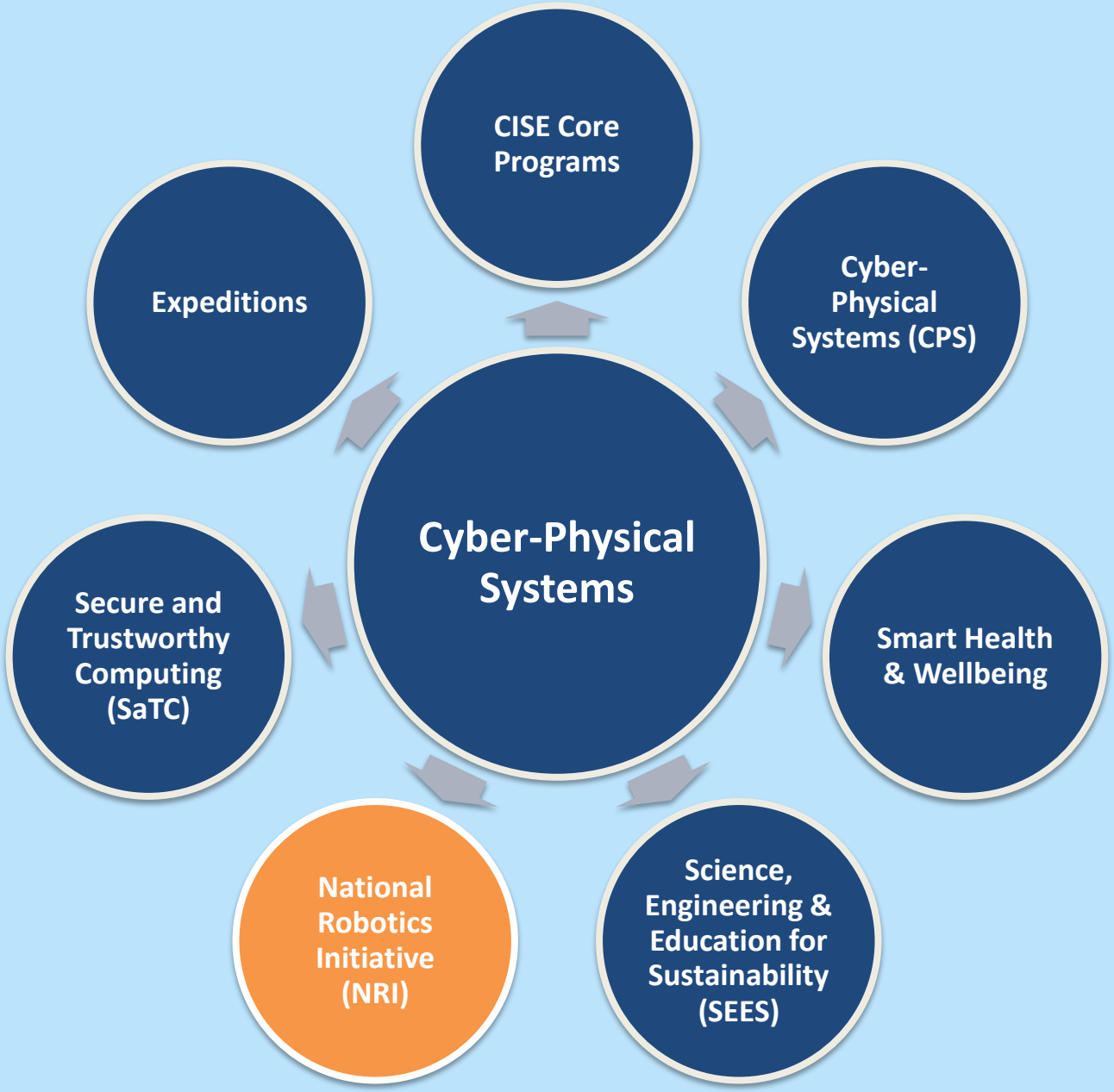
Engage the research community in developing new fundamental ideas and concepts

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

Project Types:

- **Small**
  up to $500,000
  over 3 years
- **Medium**
  up to $1,200,000
  over 4 years
- **Frontier**
  up to $10,000,000
  over 5 years

CPS Support across NSF



National Robotics Initiative (NRI)

Developing the next generation of collaborative robots to enhance personal safety, health, and productivity

A nationally concerted cross-agency program to provide U.S. leadership in science and engineering research and education aimed at the development and use of cooperative robots that work alongside people across many sectors.

Image Credit: *Bristol Robotics Lab*

Research Thrusts

- **Fundamental research in robotics science & engineering**
- **Understanding the long term social, behavioral, and economic implications across all areas of human activity**
- **Use of robotics to facilitate and motivate STEM learning across the K-16 continuum**

Cross-Directorate Program: CISE, EHR, ENG, and SBE

Multi-agency Commitment: NSF, NASA, NIH, USDA

Wrap Up

- As automation pervades new platforms, the trend toward increasingly cyber-enabled physical infrastructure introduces new security challenges – energy production, industrial control, healthcare and transportation.

- Unsafe operation can cause significant damage to life and/or property; may pose an emerging threat to national security and defense.

- Must consider both the physical aspects of the equipment and the cyber aspects of the controls, communications, and computers that run the system:
  - Cyber-physical systems have increasing complex attack surfaces: hard to identify, measure and assess potential risk
  - Overconfidence of system designers and engineers combined with overconfidence of infrastructure operators
  - We tend to underinvest in protection and overinvest in response

Wrap Up

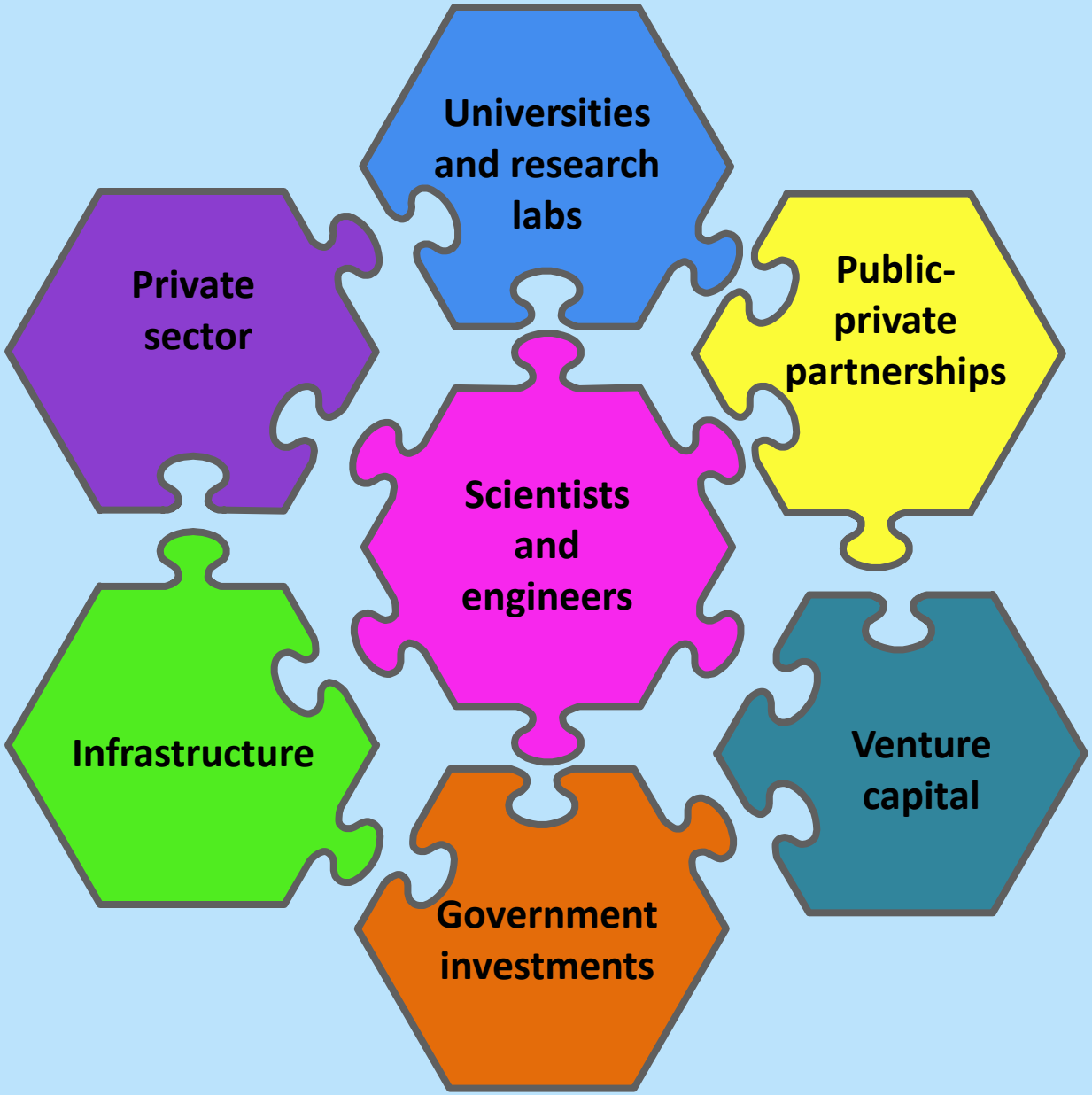
- We need to invest in a **research pipeline** (portfolio) comprising of long-term foundational research for secure cyber-physical systems, experimental prototypes, and early deployments to spur innovative applications.

- The CPS R&D community will continue to have a transformative and durable impact on our national priorities.

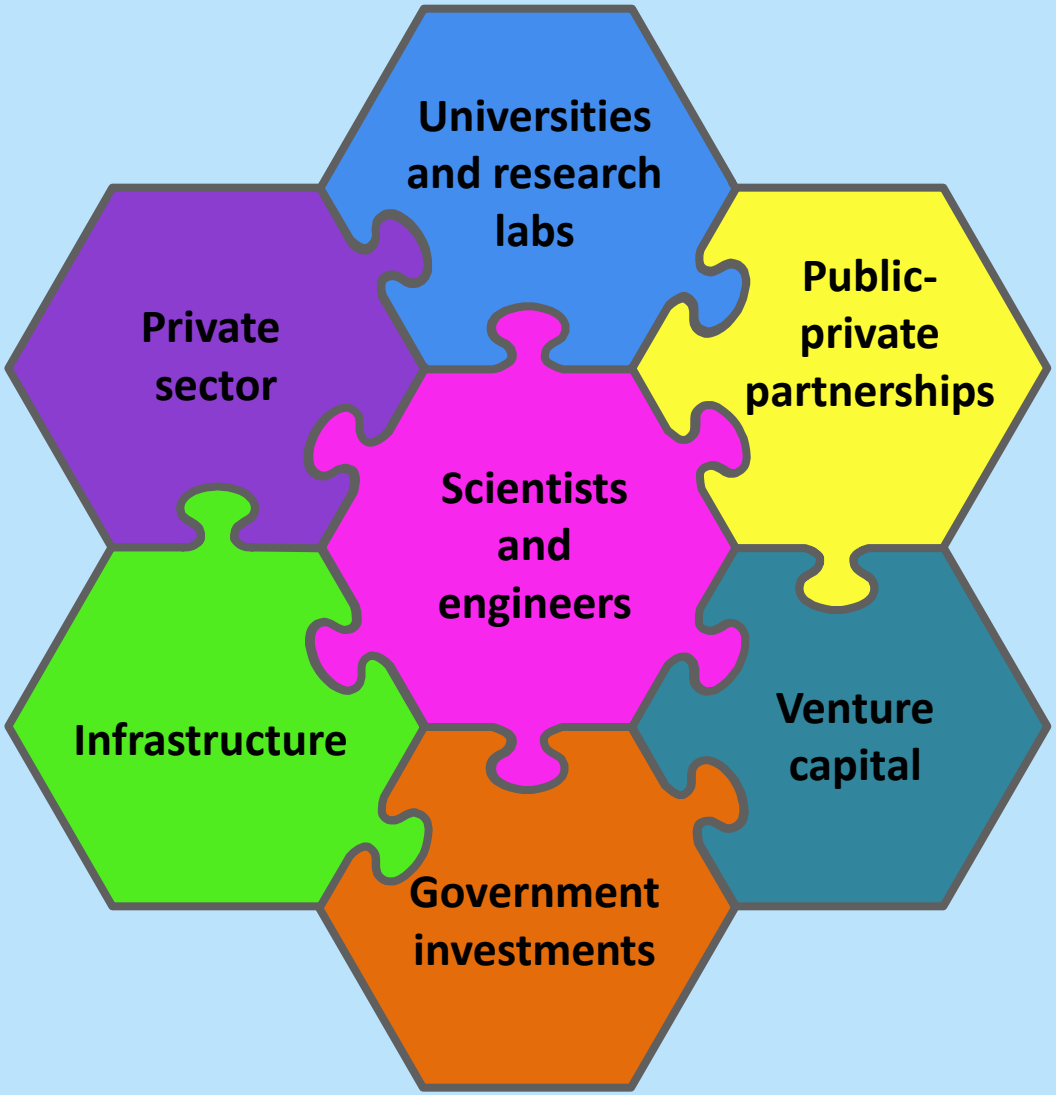
- NSF is committed to foster this emerging, consolidating research community and to reinforce its sustained role in advancing frontiers of science and engineering innovation.

- A vibrant discovery and innovation ecosystem is critical to success.

Discovery and Innovation Ecosystem



Discovery and Innovation Ecosystem



Thanks!

fjahania@nsf.gov

Credits

- Copyrighted material used under Fair Use. If you are the copyright holder and believe your material has been used unfairly, or if you have any suggestions, feedback, or support, please contact: ciseitsupport@nsf.gov.

- Except where otherwise indicated, permission is granted to copy, distribute, and/or modify all images in this document under the terms of the GNU Free Documentation license, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled “GNU Free Documentation license” http://commons.wikimedia.org/wiki/Commons:GNU_Free_Documentation_License).

- The inclusion of a logo does not express or imply the endorsement by NSF of the entities' products, services, or enterprises.