EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES

PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY

E PLURIBUS UNUM

Strategy for Cyber-Physical Resilience

Fortifying our Critical Infrastructure for a Digital World

January 2024

DRAFT/PRE-DECISIONAL

Updated 12 Jan. 2024

PCAST Working Group

PCAST Members

- Eric Horvitz (Microsoft) – *Co-Lead*
- Phil Venables (Google) – *Co-Lead*
- Jonathan Levin (Stanford)
- Bill Press (UT Austin)
- Vicki Sato (Former, Harvard)
- Lisa Su (Advanced Micro Devices)
- Kathy Sullivan (Former NOAA Admin., NASA Astronaut)

External Members:

- Richard Danzig (Former Sec. of the Navy)
- Kevin Fu (Northeastern University)
- Dan Geer (In-Q-Tel)
- George Shea (FDD)

Jonathan Levin

Vicki Sato

Bill Press

Lisa Su

Eric Horvitz

Phil Venables

Kathy Sullivan

Richard Danzig

George Shea

Kevin Fu

Dan Geer

Beyond Security: Resilience

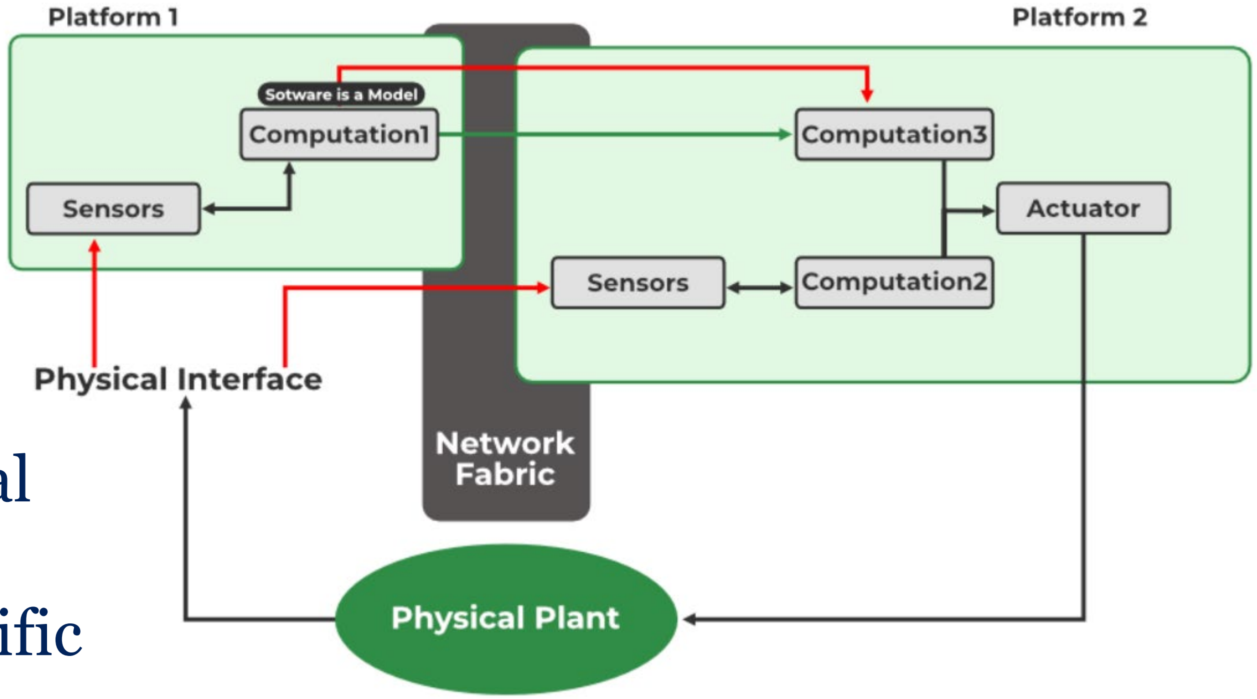
- **Focus of attention to date: *cyber-security***
- **Criticality of developing resilient systems**
- **Recommendations for action**

Our Critical Infrastructure is Cyber-Physical

- **Cyber-physical systems:** Physical systems that rely on computing technologies for sensing, analysis, tracking, controls, coordination, and communication.

- **Cyber-physical systems** underpin our infrastructure for water, energy, communications, transportation, banking, and more.

- **Cyber-physical resilience** is the capacity of an integrated cyber-physical system to keep running—even if not at peak performance—should it lose specific functions.



From: geeksforgeeks.org

Need for Cyber-Physical Resilience

Cyber-physical systems have both physical & cyber vulnerabilities and can be impacted by accidents or errors, natural disasters, and malicious attacks.

Examples

- Attack: Colonial pipeline (2021), Maersk shipping (2017)
- Natural event: Texas power (2021)
- Maintenance error: FAA (2023)

Unfortunately, protections against cyber and physical risk have developed independently.

Overarching Principles

- Complexity of cyber-physical systems underpinning our critical infrastructure requires us to cope with vulnerabilities that cannot be completely identified, much less eradicated.

- Cyber-physical risk is high, while protections are disproportionately low.
- Cyber-physical systems are often networked and depend on other cyber-physical systems that are themselves networked
- New technologies, especially AI systems, will transform the landscape of cyber-physical security, amplifying capacities for both attack and defense
- Future systems must be designed and made resilient by cyber-informed engineering from the start.

Recommendation 1: **Establish Performance Goals**

Set minimum delivery objectives for critical services, even in the face of adversity, and establish more ambitious performance goals to measure all organizations ability to achieve and sustain those objectives.

- 1A: **Define Sector Minimum Viable Operating Capabilities & Minimum Viable Delivery Objectives**

- 1B: **Establish and Measure Leading Indicators**

- 1C: **Commit to Radical Transparency and Stress Testing**

Example Minimum Viable Operating Objective & Minimum Viable Delivery Objectives

Bounded Impact: expressions of minimum delivery goals e.g.:

> *No more than 50,000 people will be without x (e.g., water, food, electricity, communications) for more than 1 week*

Bounded Failure: measure of the maximal impact of any single failure via containment of spread by creating independence and resilience of subsystems and components to failures of other components

Leading Indicators

The intent of these metrics is to identify an organization’s most critical systems. Specific metrics would be created in the context of each sector and organization.

1. *Hard Restart Recovery Time*
2. *Cyber-physical Modularity*
3. *Internet Denial / Communications Failure*
4. *Fail-over to Manual Operations*
5. *Control Pressure Index*
6. *Software Reproducibility*
7. *Preventative Maintenance Vibrancy*
8. *Inventory Completeness*
9. *Stress Testing Vibrancy (red teaming)*
10. *Common Mode Failures and Dependencies*

Recommendation 2: **Bolster and Coordinate Research and Development**

Research and development in cyber-physical resilience is fragmented and unfocused. We need to marshal our academic and private sector R&D capabilities.

- 2A: **Establish a National Critical Infrastructure Observatory**
- 2B: **Formulate a National Plan for Cyber-Physical Resilience Research**
- 2C: **Pursue Cross-ARPA and Cross-Agency Coordination**
- 2D: **Radically Increase Engagement on International Standards**
- 2E: **Embed Cyber-Physical Resilience Skills into Engineering Professions and Education Programs**

Recommendation 3: **Break Down Silos and Strengthen Government Cyber-Physical Resilience Capacity**

Clarify the what and why of the national critical functions list to help each sector prioritize. Enhance the staffing and capabilities of Sector Risk Management Organizations and the Cyber Safety Review Board so that they can perform their important roles.

- 3A: **Establish Consistent Prioritization of Critical Infrastructure**
- 3B: **Bolster Sector Risk Management Staffing and Capabilities**
- 3C: **Clarify and Strengthen Sector Risk Management Agency Authorities**
- 3D: **Enhance the DHS Cyber Safety Review Board**

Recommendation 4: **Develop Greater Industry, Board, CEO, and Executive Accountability**

Increase the expectation that boards, CEOs, and other executives, as the owners and operators of our critical infrastructure, will lead from the front. More of the private sector should augment their "tone at the top" with "resources in the ranks" to be prepared for adverse events.

- 4A: **Enhance Sector Coordinating Councils**
- 4B: **Promote Supply Chain Focus & Resilience by Design**

Conclusion

- Our national critical infrastructure is dependent on cyber-physical systems
- These systems experience attacks and accidents every day, as well as extreme events
- Move beyond defense to resilience to provide minimal viable services in the face of attacks and disruptions
- Recommendations:
  - Aim to set more ambitious performance goals moving beyond security to resilience
  - Create a more aligned R&D agenda to support those goals, including building a National Critical Infrastructure Observatory
  - Equip government agencies with more capabilities and authorities to deliver resilience
  - Stimulate the private sector owner/operators of our critical infrastructure to amplify executive level "tone at the top" and also increase "resources in the ranks"