ASU Global Security Initiative

Arizona State University

Cybersecurity in the context of global security

Nadya T. Bliss, PhD
@nadyabliss

https://globalsecurity.asu.edu

Table of contents

1 A global challenge
2 The cybersecurity imperative
3 Key investment areas
4 Summary

National Security:
An increasingly global challenge

- Cybersecurity
- Disinformation and misinformation
- Resource scarcity
- Pandemics
- The race to lead in AI

Sampling of security sector research priorities

	Intelligence Community	Dept. of Defense	Dept. of Homeland Security	Industry
Global Security Initiative Capabilities	• Advanced analytics to drive decision-making • Information manipulation • Autonomous discovery of vulnerabilities in software and firmware • Novel sensors to reveal adversary activities	• Advanced autonomous systems • Information manipulation • Resilient information networks • Improve vulnerability detection through human-machine symbiosis	• Resilient critical infrastructure • Advanced analytics to drive decision-making • Unmanned aerial systems • Novel sensors to reveal adversary activities	• Privacy and data security • Resilient information networks • Algorithmic bias

Common challenges

- Re-emergence of long-term, strategic competition
- Rapid dispersion of technology
- Technology innovation not exclusively driven by government
- New concepts of warfare and competition
- Unknown consequences of the integration and teaming of humans with technology

Challenge: Technological innovation no longer primarily driven by U.S. government

- Industry now the main innovator
- Leads to rapid dispersion of new technologies
- National security not primary concern when developing a new technology
- Market dynamics motivate industry to want to work with strategic competitors

The Cybersecurity Imperative

Avoid the tendency to let functionality alone drive development, and build in security, trustworthiness, and privacy from the start

Consider potential misuses and abuses when developing a new technology

Trustworthiness: Ensuring that the systems perform as expected

Security: Ensuring that the systems are protected from breaches

Privacy: Ensuring that the data and information collected are used as advertised with clear policy definitions for algorithmic accountability

Cybersecurity is not technology-only challenge

It is a technology + human challenge that requires interdisciplinary research and education aimed at creating tech-savvy citizens

Explainability

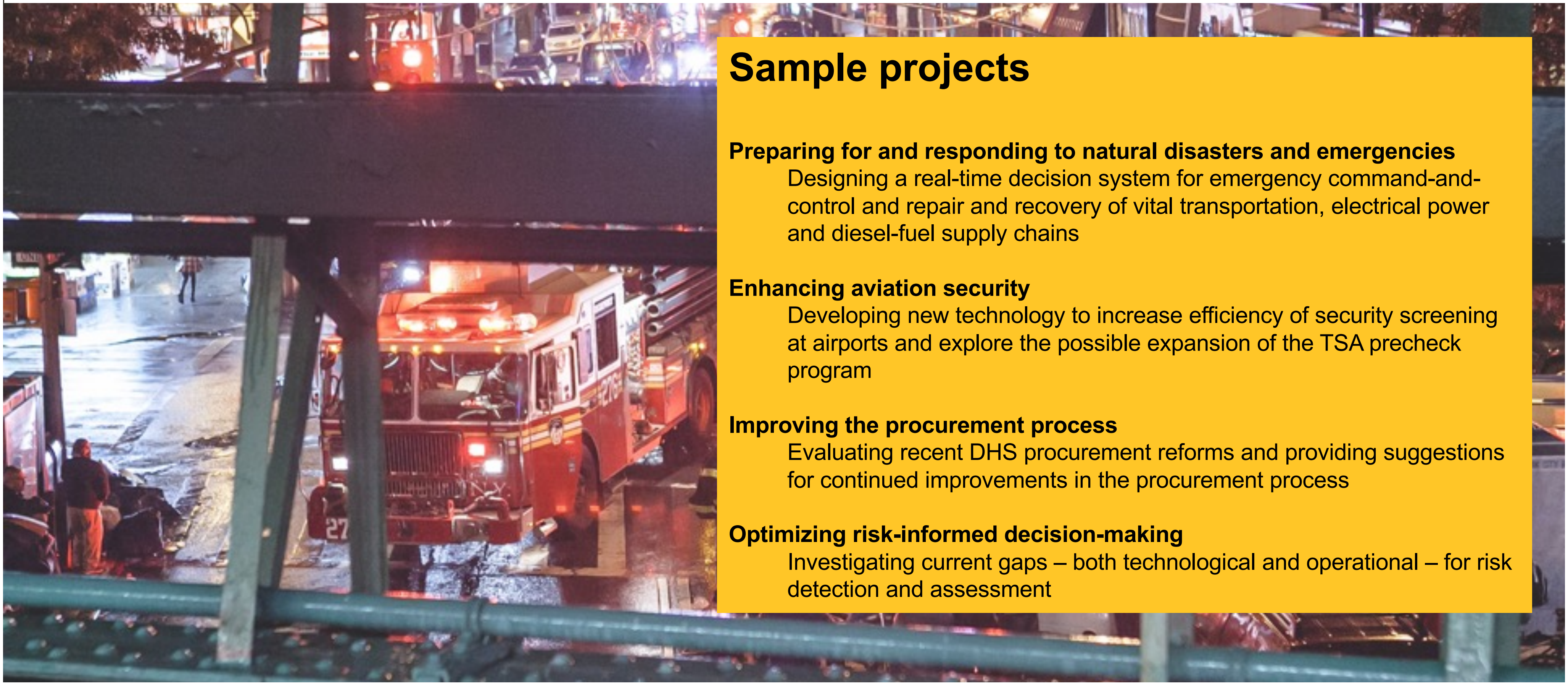
The ability to understand and explain why automated systems produce certain results

Requires investments in key research areas

- Cybersecurity
- Artificial Intelligence
- Teaming science (AI, robot and human teaming)
- Narrative framing and disinformation/misinformation
- Data and visualization

Capability:
The Center for Accelerating Operational Efficiency

A Department of Homeland Security Center of Excellence



Sample projects

Preparing for and responding to natural disasters and emergencies

Designing a real-time decision system for emergency command-and-control and repair and recovery of vital transportation, electrical power and diesel-fuel supply chains

Enhancing aviation security

Developing new technology to increase efficiency of security screening at airports and explore the possible expansion of the TSA precheck program

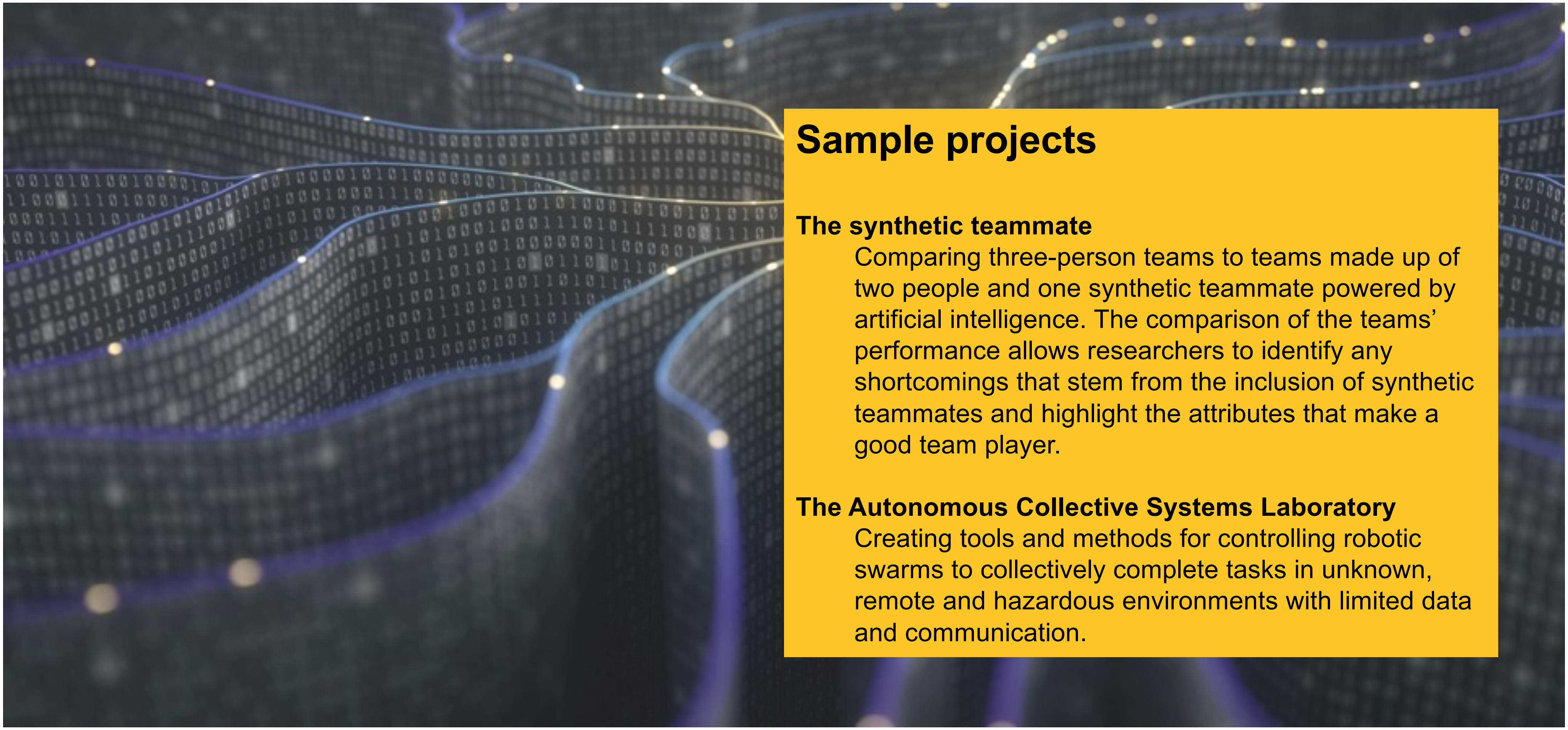
Improving the procurement process

Evaluating recent DHS procurement reforms and providing suggestions for continued improvements in the procurement process

Optimizing risk-informed decision-making

Investigating current gaps – both technological and operational – for risk detection and assessment

Capability:
The Center for Human, AI, and Robot Teaming



Sample projects

The synthetic teammate

Comparing three-person teams to teams made up of two people and one synthetic teammate powered by artificial intelligence. The comparison of the teams' performance allows researchers to identify any shortcomings that stem from the inclusion of synthetic teammates and highlight the attributes that make a good team player.

The Autonomous Collective Systems Laboratory

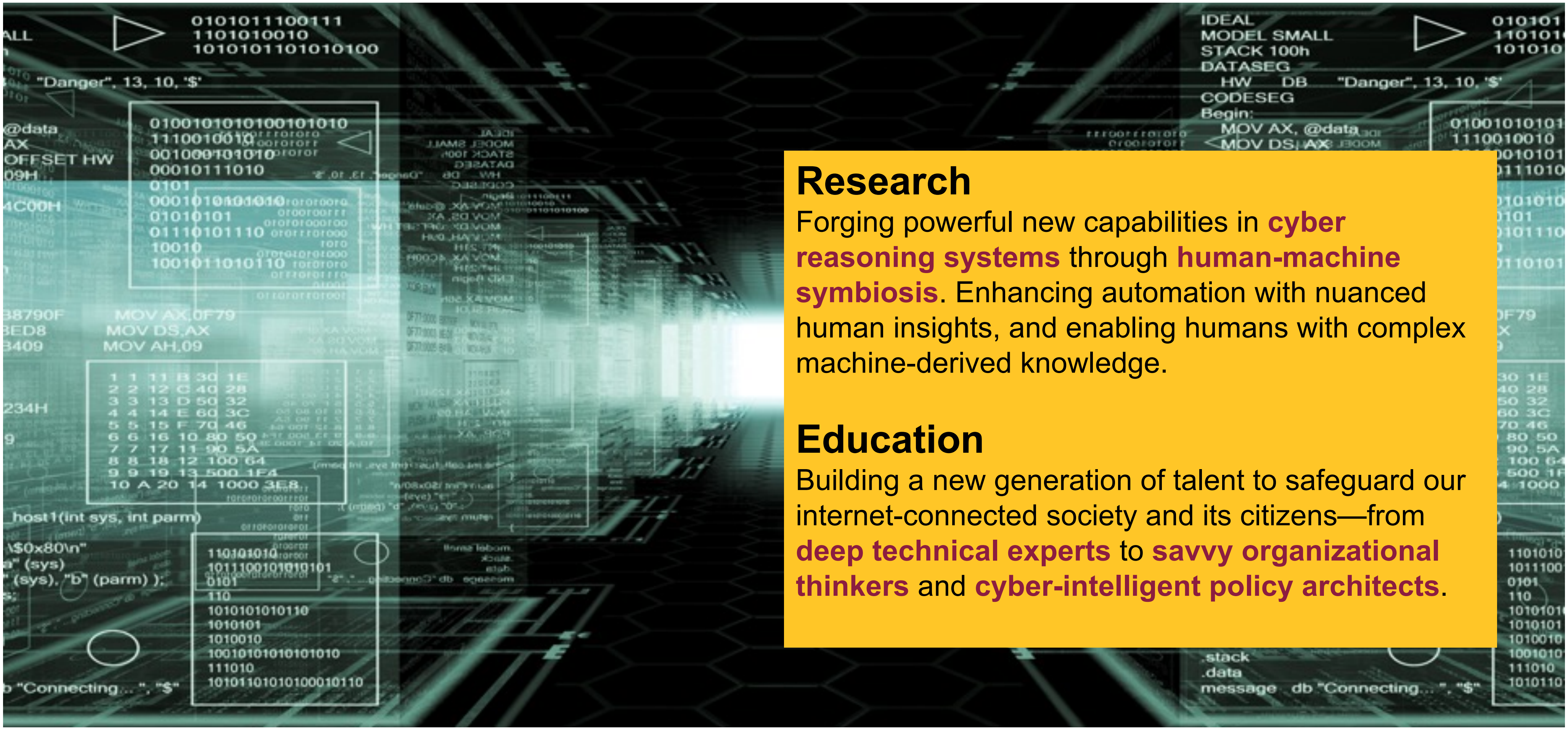
Creating tools and methods for controlling robotic swarms to collectively complete tasks in unknown, remote and hazardous environments with limited data and communication.

Capability:
Narrative and Strategic Influence

Sample project

Mapping disinformation activities in the European Theater
Developing forecasting methods to anticipate future disinformation campaigns and their likely communication vectors, targets, techniques, and procedure. The team will build this tool by researching what narratives are circulating, what framing is present that guides interpretation of facts and events, and what network structures exist to transmit information.

Capability:
The Center for Cybersecurity and Digital Forensics



Research

Forging powerful new capabilities in **cyber reasoning systems** through **human-machine symbiosis**. Enhancing automation with nuanced human insights, and enabling humans with complex machine-derived knowledge.

Education

Building a new generation of talent to safeguard our internet-connected society and its citizens—from **deep technical experts** to **savvy organizational thinkers** and **cyber-intelligent policy architects**.

Research and implementation alone are not enough

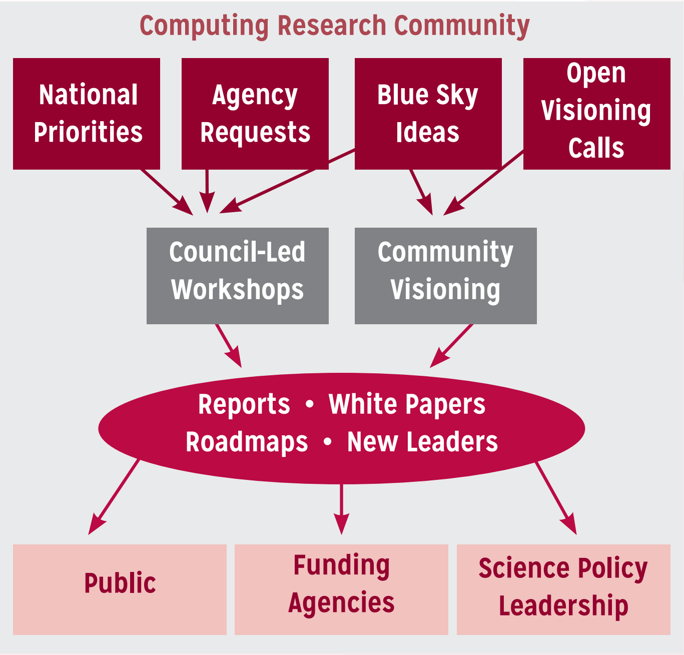
Education: As more decisions are made with the aid of automated systems, it is important that people ***understand how*** those decisions are being made

Summary

- **Today’s security challenges transcend borders**
  - The U.S. must work with allies to address these challenges
- **Interdisciplinary research is key to addressing security challenges**
  - Technology-only solutions rarely work
- **Shift from reactive cybersecurity to proactive cybersecurity**
  - Consider security concerns in the conceptual phase and through development
- **An informed and tech-savvy citizenry is crucial**
  - Requires technology that has explainability

COMPUTING COMMUNITY CONSORTIUM

CCC's mission is to catalyze the computing research community and enable the pursuit of innovative, high-impact research.



Computing Research Community

National Priorities

Agency Requests

Blue Sky Ideas

Open Visioning Calls

Council-Led Workshops

Community Visioning

Reports • White Papers

Roadmaps • New Leaders

Public

Funding Agencies

Science Policy Leadership

Who:

- Council with 20 members
- Chair, VC, & Director
- CCC/CRA Staff

Inputs: Bottom-up, Internal, & Top-Down

What:

- Workshops & Conf. Blue Sky Tracks
- Whitepapers & Social Media
- Reports Out (esp. to government)
- Biennial Symposium in DC

Talent Development

- Early Career Workshops & Participation
- Council Membership
- Leadership w/ Gov't (LISPI)

CCC 2018-2019 TASK FORCES

- **Cybersecurity and Cybercrime**
- Health and Human Computer Interaction
- **Information Integrity and Provenance**
- *Intelligent Infrastructure*
- *Fairness and Accountability*
- Systems and Architecture
- Industry Working Group on Transportation
- AI Roadmap Working Group

CCC
Computing Community Consortium
Catalyst