



erVa

NSF Engineering Research  
Visioning Alliance

# Engineering R&D Solutions for Unhackable Infrastructure

Executive Summary



## Executive Summary

Infrastructures include at least four key components that converge to deliver useful functionality: physical infrastructure, software and algorithms, data communications, and humans. The latter design, deploy, and operate infrastructure. They can also become attack agents and threats.

The goal of “unhackable infrastructure” is for the engineering research and development community to dramatically raise the bar on robust protections against an enormous array of adversarial threats across an enormous array of infrastructure domains, many of which will be new in the days ahead.

As technological advances provide more sophisticated tools and systems (e.g., artificial intelligence-driven autonomous agents, real-time automation), adversaries will be able to leverage these new technologies to expand their capabilities. This should be anticipated by the research community.

A future with unhackable infrastructure was the challenge presented to a diverse array of experts and practitioners convened by the Engineering Research Visioning Alliance (ERVA). A Thematic Task Force with members from academia, industry, and the nonprofit sectors identified five key areas for research investment to advance progress toward this aim.



Credit: Evan Dougherty/Assistant Multimedia Editor, University of Michigan, College of Engineering

# Key Areas for Research Investment

## 01

### Human-Technology Interface Considerations

- Humans are both the weakest link in security and the greatest opportunity to advance protections in cyber-physical infrastructure.
- Research should greatly increase focus on the human element within tomorrow's infrastructure; for example, including humans in system security modeling and addressing the incentives and the economics surrounding adversarial behavior and security design.

## 02

### Measuring and Verifying Security (Metrics)

- Advances in measurement tools and metrics for tomorrow's infrastructures are sorely needed to support security risk evaluation, design tradeoffs, verification, automation, and more.
- Additional tools are needed to support observability, autonomous attack recovery, and designed-in verification techniques.

## 03

### Future Approaches to Autonomous Security

- Autonomous security (self-configuring, self-guiding, self-managing, self-learning, self-tuning, etc.) is needed to address both complexity and scale in tomorrow's infrastructures.
- Autonomous agents addressing security functionality could be used in service of, or in synergy with, human decision-makers.
- Autonomous systems need better contextual understanding and response capabilities.



## 04

### **New Approaches to Resilience in Interdependent Infrastructures**

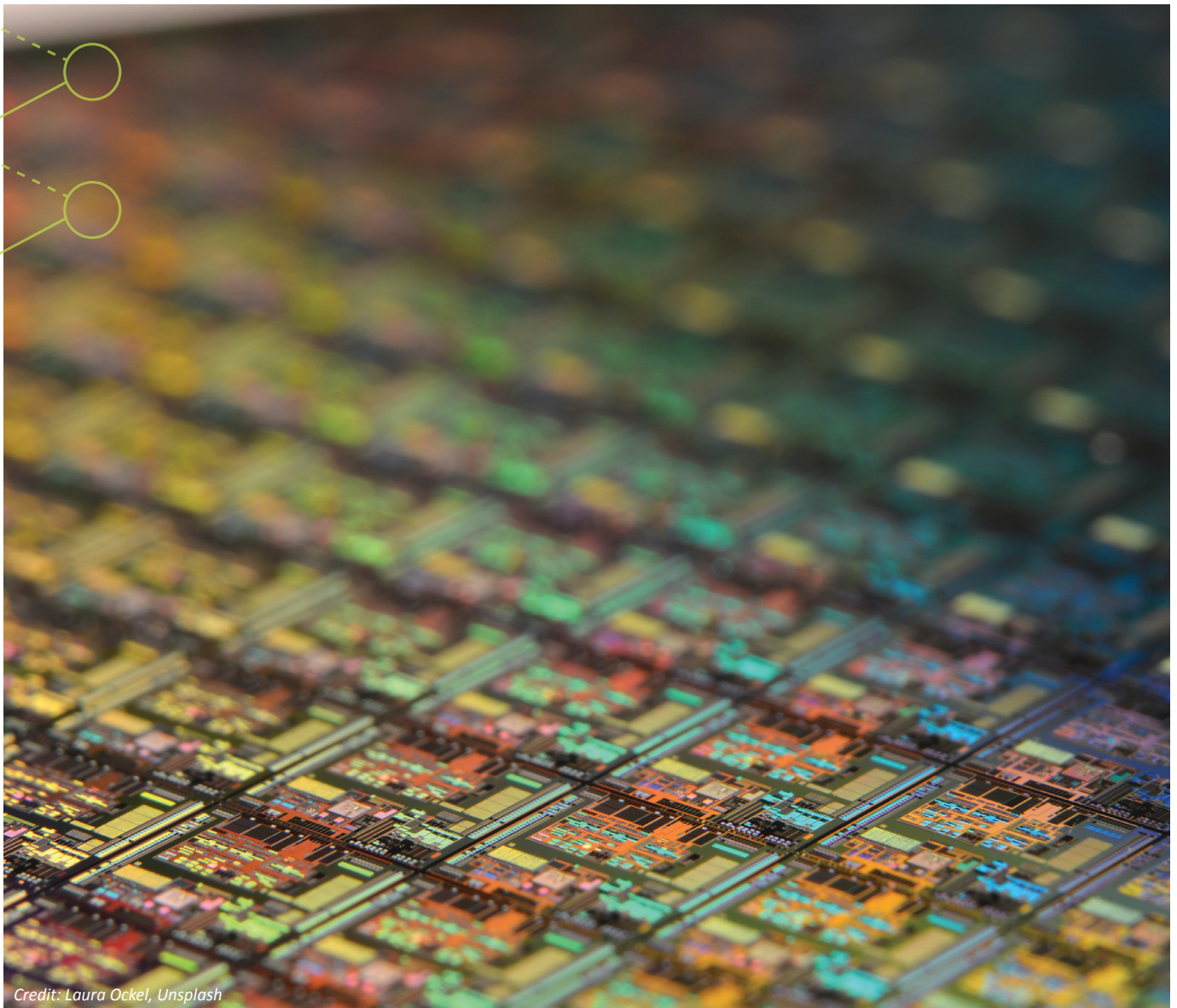
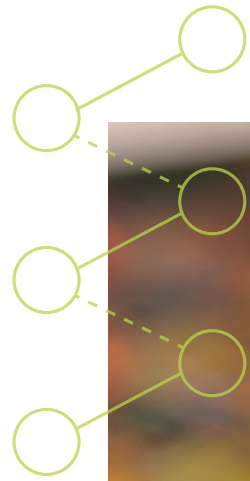
- Attackers are becoming more adept at exploiting the vulnerabilities of hierarchically managed infrastructures with tightly coupled processes and complex dependencies.
- An important opportunity for future research is to develop design approaches that maintain system-level properties of safety and security after the integration of modular components.

## 05

### **Architecting Trustworthy Systems**

- Research in trustworthy systems architectures looks at how correctness of operation can be verified more robustly and built into system architectures and infrastructure.
- Some key issues include design specification, decentralized control, confidential computing, and new infrastructure domains.

THE RESEARCH PRIORITIES DETAILED IN THIS REPORT LAY THE GROUNDWORK FOR A FUTURE WITH UNHACKABLE INFRASTRUCTURE.



*Credit: Laura Ockel, Unsplash*

## Taking Action

Anticipating and preparing for security threats, whether short-, medium-, or long-term, has escalated as a critical national and international priority. Engineering-led research and innovation is needed to lay the foundation for tomorrow's solutions in cybercrime prevention, especially as systems become an increasingly complex co-mingling of physical and cyber components.

Every focus area selected by the Thematic Task Force provided opportunities to progress toward the ideal of infrastructure through proactive and comprehensive research approaches. The aim of this report is to inspire researchers and sponsors (public, private, and nonprofit) to pursue these priorities. ERVA challenges readers to disseminate this report and prioritize areas with potential for the greatest return on investment.



NSF Engineering Research  
Visioning Alliance

Our mission is to identify and develop bold and transformative new engineering research directions and to catalyze the engineering community's pursuit of innovative, high-impact research that benefits society.



ERVA IS FUNDED BY THE NATIONAL SCIENCE FOUNDATION THROUGH  
AWARD NUMBER 2048419

©2022 Engineering Research Visioning Alliance. All rights reserved.

*This material is based upon work supported by the National Science Foundation under Grant # 2048419. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.*

[Ervacommunity.org](http://Ervacommunity.org)