CCC's response to the [Networking and Information Technology Research and Development Request for Information on a National Plan for Cyber-Physical Systems Resilience]

This response is prepared by the Computing Research Association (CRA)'s Computing Community Consortium (CCC). CRA is an association of over 270 North American computing research organizations, both academic and industrial, and partners from six professional computing societies.

The mission of the CCC, a subcommittee of CRA, is to enable the pursuit of innovative, high-impact computing research that aligns with pressing national and global challenges. Please note any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the authors' affiliations, or of the National Science Foundation, which funds the CCC.

This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in the National Cyber-Physical Systems Resilience R&D Strategic Plan and associated documents without attribution.

October 26, 2024

Written by: *Gabrielle Allen (University of Wyoming), David Danks (University of California, San Diego), Catherine Gill (Computing Community Consortium), and Katie Siek (Indiana University).*

To ensure the National Plan for Cyber-Physical Systems Resilience Research is thorough and advantageous to the nation, the Computing Community Consortium presents the following recommendations.

1. Prioritize Cyber-Physical-Human Resilience Efforts

Resilience of cyber-physical systems is not just about the software or infrastructure on which a system depends; it also involves the people who design, develop, operate, and

maintain every aspect of these systems. The national plan should consider human operators as distinct components in cyber-physical resilience planning. Redundancies in cyber-physical systems are key to maintaining a level of operability during crises, and similar redundancies must also be ensured at the human level (e.g., redundancies in knowledge and expertise). Systems also often lack adequate monitoring and sensing on the human side, in contrast with cyber and physical components, even though human decisions and actions can significantly impact these systems' operations. Research should explore how humans interact with systems and the potential for human error, burnout, and adaptation in crisis situations. Research should also be conducted to discover optimal triage methods for a given cyber-physical system during crises to ensure threats are managed quickly, rather than exacerbated, by on-site workers. Monitoring devices and artificial intelligence may be useful to assist humans with time critical decisions, and research into how best to use these technologies should be pursued and included in the plan.

To design cyber-physical-human systems with *all* stakeholders in mind, the strategic plan should emphasize the need to train scholars from historically excluded groups. Based on our experiences, we emphasize that institutions should be required to have checks and balances to ensure people from historically excluded groups are provided with real research experiences and treated ethically. This could be done with comparative pre-, mid-, and post-research experience surveys with one data group to make comparison reports. To further support the pipeline of future researchers, we recommend funding summer research programs for MS students, particularly those in intensive short-term programs, who often lack the opportunity to gain research experience. Moreover, the agency should require funded institutions to document their efforts in fostering an inclusive environment, with clear metrics to assess and improve the institutional culture. By doing so, the agency can shift the responsibility of addressing hostile environments from underrepresented groups to institutional leaders, ensuring that the burden is on institutions to create a supportive and welcoming atmosphere for all cyber-physical systems researchers.

2. Open Source Software and Cyber-Physical Resilience

The strategic plan should carefully evaluate the role of open-source software and tools in cyber-physical systems. Open source software can accelerate innovation, but it also presents unique security challenges. As we've seen recently, even a reputable open-source system used by leading US based companies, significant portions of the US government, and hundreds of millions of computers around the world can be susceptible to cyberattacks[1]. It is important to identify where open-source solutions can be securely integrated into critical infrastructure while ensuring proper testing and

[1] https://www.nytimes.com/2024/04/03/technology/prevent-cyberattack-linux.html

validation of code, including AI-generated software. For open-source systems which are widely used across the US and the world, mechanisms must be introduced to reduce the effectiveness of cyberattacks and staunch the bleeding when a given attack is detected.

3. The "System of Systems" Challenge

Many modern cyber-physical-human systems are composed of hundreds or even thousands of individual software systems. Each of these systems can be prone to failure or vulnerable to attacks in a myriad of diverse ways, but a focus solely on individual components is insufficient. In particular, interdependencies between systems must also be accounted for. Digital twins and other simulation tools can be used to model the behavior of interconnected systems, including human roles. These tools can help identify failure modes and the cascading effects of disruptions across different sectors. In addition, standards for testing resilience across multiple domains (e.g., physical, cyber, human) must be established. Recommendations for continuous testing and verification should be included in the national plan, especially as systems evolve and new AI-driven capabilities are added.

4. Incentivize Resilience and Resilience Research

A key difficulty in establishing a resilient digital ecosystem is the need for consistent enforcement. These systems are inherently interconnected, which poses a challenge to both prevention and isolation of breaches. Without universal enforcement of cybersecurity and resilience standards, a system can be left as vulnerable as the weakest link. Further, the stakeholders in the digital economy are diverse; simple government fiat is not sufficient to ensure compliance, absent a strong and efficient enforcement mechanism. Participants in the digital economy need an incentive to take these threats and challenges seriously.

There is an obvious solution to this issue. By making participants in the digital economy liable for damages caused by their security and resilience negligence, the government can ensure standards are immediately taken seriously. The potential damages for failure are massive, and to balance the risk of a breach or problem, economic actors would need to carry insurance against failures. In turn, insurance companies would promulgate security and resilience standards in line with the expectations of regulators. This system would work similarly to car, home, and malpractice insurance, where it is not direct government oversight driving compliance, but a self-interested insurance industry protecting against the risk of economic liability.

Additionally, efforts to holistically evaluate and overhaul cyber-physical systems will be expensive and require dedicated long-term funding to continue to test and evaluate

systems as threats and attack methods evolve. We recommend funding fewer projects that are threat-agnostic and can be utilized to improve many cyber-physical systems. This can include projects like creating robust datasets for modeling and testing resilience, similar to successful initiatives in medical research. Funding threat-agnostic approaches can maximize flexibility in responding to emerging threats, including those that are unanticipated. The national plan should also recommend utilizing existing research centers and federal laboratories to spearhead resilience testing and experimentation, with a particular focus on critical infrastructure. Federally funded projects which aim to develop cyber-physical systems should have requirements for developing robust systems. These projects could also require the development of maintenance and testing plans to implement following the deployment of these systems.

5. Collaborate with Researchers

The PCAST report references the need to establish minimum operating capacities for critical systems to maintain essential functions during crises. This report mentions several government agencies which should assist in carrying out this task, such as NIST, however, it does not mention the important role that researchers will play. Engaging the research community in defining these capabilities would ensure they are realistic and robust.