The Great Cybersecurity Reset

Dr. Ron Ross
Fellow, Dartmouth College
Institute for Security, Technology, and Society

Great national challenges require great national solutions.

In 1961, Americans perceived that the United States was losing the space race with the Soviet Union. This situation was deemed unacceptable as it represented a potential existential kinetic threat to national and economic security. On September 12, 1962, President John F. Kennedy in one of his most memorable speeches, challenged the Nation with his bold "moon landing" proposal.

The speech was strategic; it was visionary; and it challenged the best and the brightest of the American people in government, industry, and academia to do something that had never been done before. It was the best example of what I refer to as “the essential partnership.”

> *“We choose to go to the Moon in this decade and do the other things, not because they are easy, but because they are hard; because that goal will serve to organize and measure the best of our energies and skills, because that challenge is one that we are willing to accept, one we are unwilling to postpone, and one we intend to win.”*

Fast forward to 2025.

We have a *new* existential threat to our nation. This threat involves our computing systems — many of which are deeply embedded in the U.S. critical infrastructure including the defense industrial base, energy, communications, critical manufacturing, transportation, healthcare, financial services, nuclear, emergency services, food and agriculture, water, and information technology. Recent Congressional testimony from a former White House Cybersecurity Coordinator provides an excellent summary of the cyber threat and the sense of urgency for action.

> *"The PRC [Peoples Republic of China] is conducting a comprehensive cyber campaign against the United States, and our current defenses are not keeping pace. Chinese state hackers prepositioned malware within our power grids, pipelines, water treatment plants, and other critical infrastructure. They tapped into our telecommunications to spy on us, stole the innovations of technological research and breached the cloud systems holding government emails. They even unfairly exploit our open markets to achieve a growing advantage inside the technology we rely upon for our communications. After a decade of using cyber to steal industrial and military secrets, they've evolved to far more threatening penetrations of our nation's infrastructure."*

For the past half century, we have made significant advancements in cybersecurity due to the tireless efforts of many dedicated professionals in government, industry, and the academic community. However, our cybersecurity advancements and solutions have been largely tactical in nature and lacked a strategic focus. As systems became more complex, interconnected, and totally dependent on computing technologies with untrustworthy software, firmware, and hardware components, adversaries continued to find ways to exploit a rapidly increasing number of known and "zero-day" vulnerabilities.

So, how do we capitalize on what has worked, recognize where current processes, procedures, and approaches have fallen short, and build a long-term, strategic approach to protecting our critical technologies, systems, components, and services?

Push the cybersecurity reset button.

The ***Great Cybersecurity Reset*** involves developing an ecosystem focused on trustworthy secure systems engineering. It requires strong national leadership, strategic vision, measurable execution, and effective feedback loops to facilitate continuous improvement. There are 6 strategic pillars that comprise the ecosystem:

- A mission-focused, trustworthy secure systems engineering (TSSE) approach
- Security design principles, concepts, and best practices
- Experimental test beds of real-world systems using a TSSE approach and security design principles, concepts, and best practices
- Incubators of TSSE talent being developed within educational institutions
- Institutions that store and share TSSE experimentation results
- Technology transfer to all communities of interest

Figure 1 illustrates the 6 key pillars of the TSSE ecosystem.

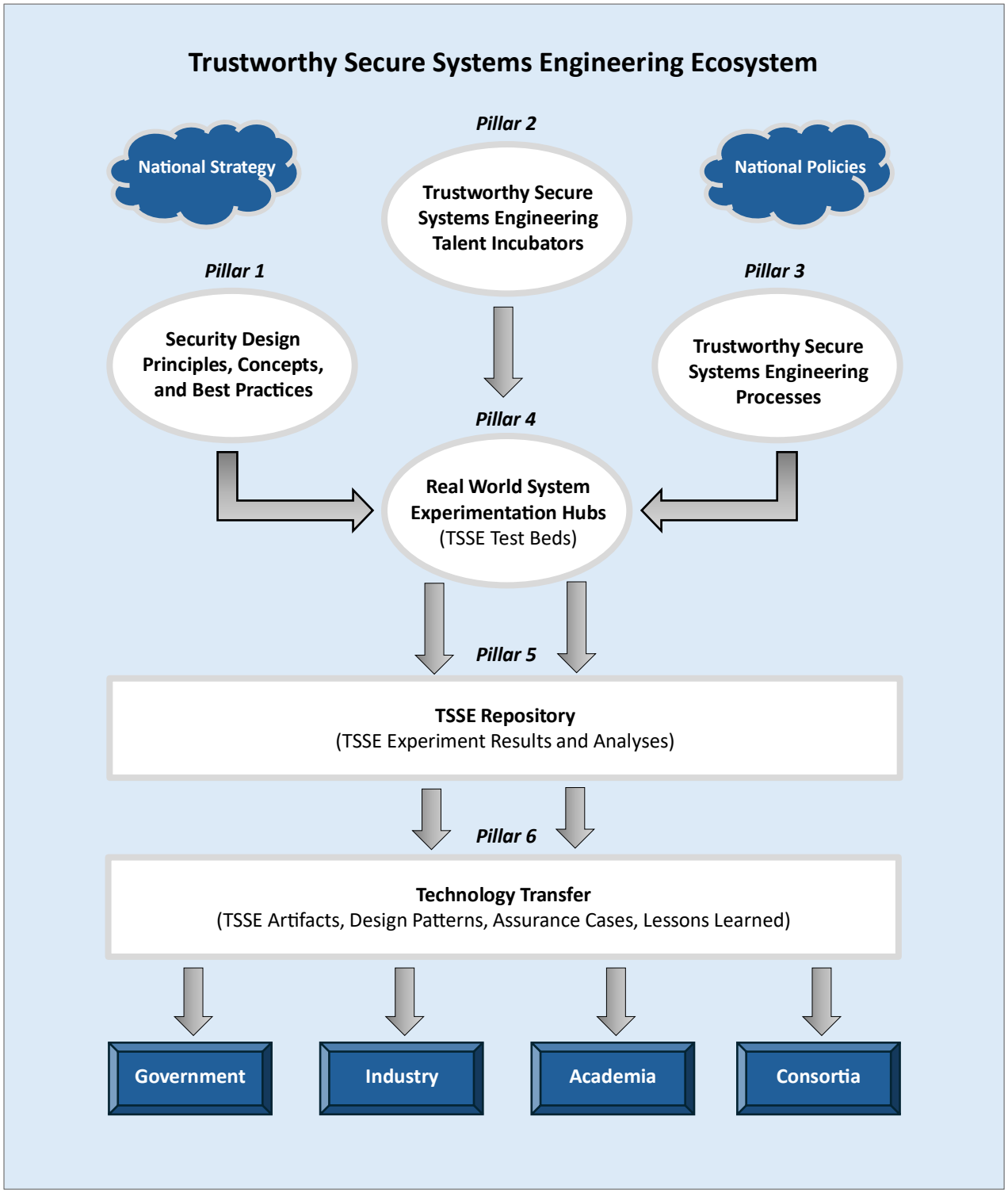

Figure. 1

You can't cobble together untrustworthy system components and expect to have systems that can be trusted to behave as intended — systems that don't go off the rails and exhibit unintended behaviors with potential catastrophic consequences. Security is like safety, reliability, and resilience. It is a "system" property that emerges from a systems engineering process informed by security design principles, concepts, and best practices — and executed within a rigorous system development life cycle process.

Engineering Trustworthy Secure Systems is not just an abstract idea. It is grounded in the fundamentals of systems engineering, computer science, mathematics, and computer security.

The Institute for Science, Technology and Society (ISTS) at Dartmouth College will be leading an effort to build an enduring framework for the ecosystem to support trustworthy secure systems engineering. A series of white papers describing each of the proposed pillars in the ecosystem will be published at a later date and posted on the ISTS website.

Join the "Ensurgency."
https://ists.dartmouth.edu