The Role of Universities in Preparing the Next Generation of Infrastructure Professionals

George H Baker, James Madison University

Available at: https://works.bepress.com/george_h_baker/10/
The Role of Universities in Preparing The Next Generation of Infrastructure Professionals

George H. Baker, Ph.D.
Institute for Infrastructure and Information Assurance
James Madison University

Highly efficient, complex, and interdependent infrastructure systems including electric power, telecommunications, transportation, water utilities, food distribution, housing and shelter, public health, finance and banking are foundations of modern societies. Over the last 3 years, the United States has become acutely aware of the importance of civil infrastructures and their criticality to the nation’s economy and quality of life. Our reliance on these systems makes them especially attractive targets for attack. Both cyber and physical attacks are known to cause major disruptions of the sometimes-fragile systems. The incidence and cost of natural disasters has also increased in recent years. The systems are so complex that we still have much to learn about their failure modes and the cascading effects caused by their elaborate interdependencies. Failure consequences can be extremely severe. Exercises simulating major infrastructure disruptions point to consequences ranging from widespread loss of critical services to the breakdown of national governance.

Universities need to play a central role in infrastructure assurance but have not yet realized their full potential. To date, we have done a good job of addressing cyber security as evidenced by the large number of world-class information security centers and degree programs producing competent information security professionals. There are now more than 50 national centers of excellence in information security education. Information security degree programs, both resident and on-line, are available at many of these institutions through the Ph.D. level. Universities are also involved in real-time assistance vis-à-vis cyber incidents with operating emergency response centers at several universities (Carnegie Mellon, USMA, Indiana, and Wisconsin as examples).

There is no doubt that cyber security is important because of the ubiquitous nature of our information networks, providing the nervous system pathways within and among most critical infrastructures. However, we need to come to grips with the challenges posed by the larger problem set of infrastructure assurance. Cyber security is an important part of the equation, albeit a subset. A balanced approach to infrastructure assurance is needed in addressing physical and cyber concerns.

R.G. Little, Director of the National Research Council Board on Infrastructure contents that existing infrastructure managers must routinely synthesize information from a broad range of disciplines including civil engineering, materials science, government operations, economics and finance, social and political science, and environmental science. Civil engineers are competent to deal with the technical/physical aspects of infrastructure issues but aren’t trained in relating technical issues in complex public forums. Public administrators in most cases lack the technical background needed to evaluate technical solutions to public needs. The challenge is the sheer complexity of infrastructure from technical, financial, and socio-political standpoints and the multidisciplinary skills

(Continued, Page 15)
Role of Universities (Cont. from Page 2) required for infrastructure planning, development, operation, and evaluation. There is a strong argument for the development of a new, dedicated infrastructure track that integrates public administration and technical disciplines to provide the balanced skill set expressly designed for infrastructure practitioners.2

While the first role of universities is education, our role in infrastructure assurance does not stop there. University infrastructure assurance programs should embrace research, policy studies, public awareness, development and promulgation of best practices, and real-time/real-problem assistance to public and private infrastructure stakeholders. Universities, as trusted agents, are capable of gathering data and assisting infrastructure service providers that are often reluctant to work with government organizations.

Universities can lead by example since they represent microcosms of critical infrastructure networks and system interdependencies. The campus provides an excellent location for developing and demonstrating infrastructure assurance practices and tools. And universities are one of the most challenging venues vis-a-vis infrastructure assurance given the openness needed for academic pursuits. Thus the university example advances state-of-the-art approaches to achieving security while at the same time protecting the freedom of the individual. If we can effectively protect university infrastructure, we can apply the lessons learned to secure many other types of open institutions.

As an example, James Madison University is developing a broad program that combines infrastructure and cyber assurance activities, leveraging our established information security program. We seek to cultivate a balanced ensemble of cyber and physical pursuits contributing to infrastructure assurance. To coordinate many diverse, interdisciplinary contributing activities within the University, we have established a new Institute for Infrastructure and Information Assurance (IIIA). The institute administers activities of two major grants, the Critical Infrastructure Protection (CIP) federal grant in partnership with George Mason University, and the (Virginia) Commonwealth Information Security Center (CISC) grant. We have begun developing new curricula in the infrastructure assurance discipline beginning with an infrastructure survey course and moving toward an information analyst track. Under the CIP project, we are developing new infrastructure network risk assessment tools at the same time engaging in actual system risk assessments to ensure the usefulness of the tools. Our risk assessment clients presently include university network IT operations and a local municipal electric power system, both efforts tightly coupled with the risk tool development. We are providing public awareness through visiting scholar forums and awareness presentations to local public service organizations. Our research program includes projects that span the prevention, protection and response infrastructure and information assurance strategies. Research is geared to foster the participation of both graduate and undergraduate students.

Addressing infrastructure issues as an explicit university program including instruction and research provides opportunities to develop and coordinate new and innovative programs that emphasize interdisciplinary thinking, communication, team building, and problem solving. We must break down the barriers separating the hard sciences, law, public policy, business and economics to develop new knowledge and collaborative research venues to successfully prepare the next generation of infrastructure professionals. 3

1 National Security Agency: List of Centers of Academic Excellence in Information Security
2 R.C. Little, Educating the Infrastructure Professional: A New Curriculum for a New Discipline, National Research Council