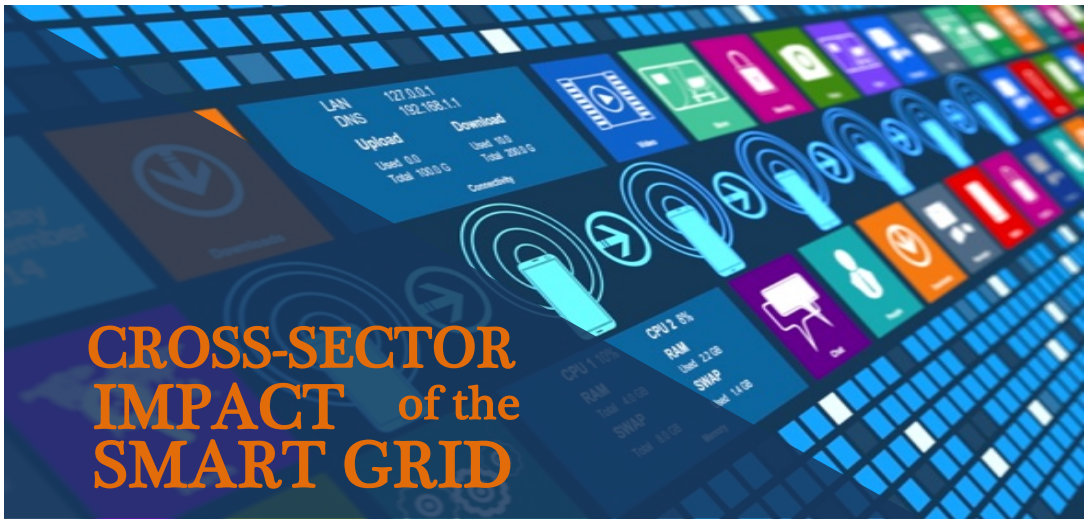
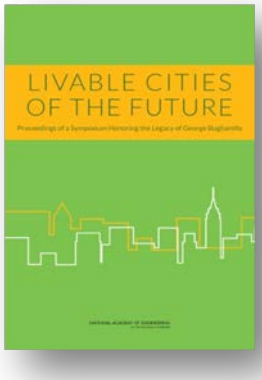


Government-University-Industry Research Roundtable
February 9-10, 2015 ▪ Washington, D.C.
List of selected reports from the National Academies related to the meeting topic: the Smart Grid

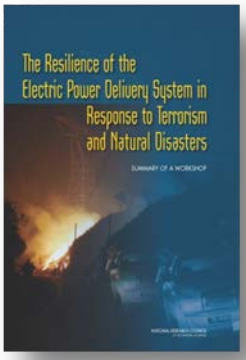
At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues (DEPS, 2014)

At the Nexus of Cybersecurity and Public Policy offers a wealth of information on practical measures, technical and nontechnical challenges, and potential policy responses. According to this report, cybersecurity is a never-ending battle; threats will evolve as adversaries adopt new tools and techniques to compromise security. Cybersecurity is therefore an ongoing process that needs to evolve as new threats are identified. *At the Nexus of Cybersecurity and Public Policy* is a call for action to make cybersecurity a public safety priority. For a number of years, the cybersecurity issue has received increasing public attention; however, most policy focus has been on the short-term costs of improving systems. In its explanation of the fundamentals of cybersecurity and the discussion of potential policy responses, this book will be a resource for policy makers, cybersecurity and IT professionals, and anyone who wants to understand threats to cyberspace.

Livable Cities of the Future: Proceedings of a Symposium Honoring the Legacy of George Bugliarello (NAE, 2014)



Livable Cities of the Future, a symposium honoring the legacy of George Bugliarello, was hosted October 26, 2012, by the Polytechnic Institute of New York University (NYU-Poly) in the Pfizer Auditorium of the Bern Dibner Library of Science and Technology. The event brought together more than 200 engineers, civic leaders, educators, and futurists to discuss how George Bugliarello's vision manifests itself in innovative urban planning for the cities of tomorrow. This report is a summary of the presentations and discussion at that event. The symposium objectives were to cultivate ideas for best practices and innovative strategies for sustainable urban development and to facilitate the evolution of New York City to a real-life laboratory for urban innovation. Participants heard the perspectives and experiences of representatives from private and public service operators, infrastructure agencies, and the academic community. Elected officials and other stakeholders in urban and other sectors examined issues critical to resilient and sustainable cities, such as energy, water supply and treatment, public health, security infrastructure, transportation, telecommunications, and environmental protection.

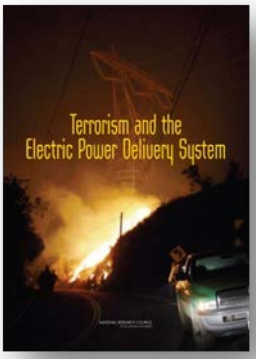


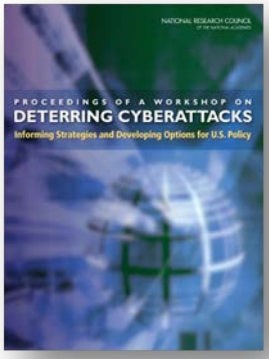
The Resilience of the Electric Power Delivery System in Response to Terrorism (DEPS, 2013)

The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters is the summary of a workshop convened in February 2013 as a follow-up to the release of the National Research Council report *Terrorism and the Electric Power Delivery System*. That report had been written in 2007 for the Department of Homeland Security, but publication was delayed because of security concerns. While most of the committee's findings were still relevant, many developments affecting vulnerability had occurred in the interval. The 2013 workshop was a discussion of the committee's results, what had changed in recent years, and how lessons learned about the grid's resilience to terrorism could be applied to other threats to the grid resulting from natural disasters. The purpose was not to translate the entire report into the present, but to focus on key issues relevant to making the grid sufficiently robust that it could handle inevitable failures without disastrous impact. The workshop focused on five key areas: physical vulnerabilities of the grid; cybersecurity; mitigation and response to outages; community resilience and the provision of critical services; and future technologies and policies that could enhance the resilience of the electric power delivery system.

Terrorism and the Electric Power Delivery System (DEPS 2012)

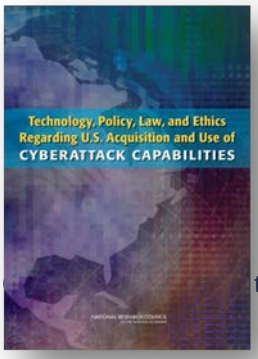
The electric power delivery system that carries electricity from large central generators to customers could be severely damaged by a small number of well-informed attackers. The system is inherently vulnerable because transmission lines may span hundreds of miles, and many key facilities are unguarded. This vulnerability is exacerbated by the fact that the power grid, most of which was originally designed to meet the needs of individual vertically integrated utilities, is being used to move power between regions to support the needs of competitive markets for power generation. Primarily because of ambiguities introduced as a result of recent restricting the of the industry and cost pressures from consumers and regulators, investment to strengthen and upgrade the grid has lagged, with the result that many parts of the bulk high-voltage system are heavily stressed. *Terrorism and the Electric Power Delivery System* focuses on measures that could make the power delivery system less vulnerable to attacks, restore power faster after an attack, and make critical services less vulnerable while the delivery of conventional electric power has been disrupted.





Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (DEPS, 2010)

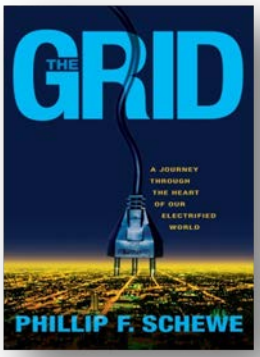
In a world of increasing dependence on information technology, the prevention of cyberattacks on a nation's important computer and communications systems and networks is a problem that looms large. Given the demonstrated limitations of passive cybersecurity defense measures, it is natural to consider the possibility that deterrence might play a useful role in preventing cyberattacks against the United States and its vital interests. At the request of the Office of the Director of National Intelligence, the National Research Council undertook a two-phase project aimed to foster a broad, multidisciplinary examination of strategies for deterring cyberattacks on the United States and of the possible utility of these strategies for the U.S. government. The first phase produced a letter report providing basic information needed to understand the nature of the problem and to articulate important questions that can drive research regarding ways of more effectively preventing, discouraging, and inhibiting hostile activity against important U.S. information systems and networks. The second phase of the project entailed selecting appropriate experts to write papers on questions raised in the letter report. A number of experts, identified by the committee, were commissioned to write these papers under contract with the National Academy of Sciences. Commissioned papers were discussed at a public workshop held June 10-11, 2010, in Washington, D.C., and authors revised their papers after the workshop. Although the authors were selected and the papers reviewed and discussed by the committee, the individually authored papers do not reflect consensus views of the committee, and the reader should view these papers as offering points of departure that can stimulate further work on the topics discussed. The papers presented in this volume are published essentially as received from the authors, with some proofreading corrections made as limited time allowed.



Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities (DEPS 2009)

The United States is increasingly dependent on information and information technology for both civilian and military purposes, as are many other nations. Although there is a substantial literature on the potential impact of a cyberattack on the societal infrastructure of the United States, little has been written about the use of cyberattack as an instrument of U.S. policy. Cyberattacks--actions intended to damage adversary computer systems or networks--can be used for a variety of military purposes. But they also have application to certain missions of the intelligence community, such as covert action. They may be useful for certain domestic law enforcement purposes, and some analysts believe that they might be useful for certain private sector entities who are themselves under cyberattack. This report considers all of these applications from an integrated perspective that ties together technology, policy, legal, and ethical issues. Focusing on the use of cyberattack as an instrument of U.S. national policy, Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities explores important characteristics of cyberattack. It describes the current international and domestic legal structure as it might apply to cyberattack, and considers analogies to other domains of conflict to develop relevant insights. Of special interest to the military, intelligence, law enforcement, and homeland security communities, this report is also an essential point of departure for nongovernmental researchers interested in this rarely discussed topic.

The Grid: A Journey Through the Heart of Our Electrified World (Phillip F. Schewe 2007)



The electrical grid goes everywhere -- it's the largest and most complex machine ever made. Yet the system is built in such a way that the bigger it gets, the more inevitable its collapse. Named the greatest engineering achievement of the 20th century by the National Academy of Engineering, the electrical grid is the largest industrial investment in the history of humankind. It reaches into your home, snakes its way to your bedroom, and climbs right up into the lamp next to your pillow. At times, it almost seems alive, like some enormous circulatory system that pumps life to big cities and the most remote rural areas. Constructed of intricately interdependent components, the grid operates on a rapidly shrinking margin for error. Things can -- and do -- go wrong in this system, no matter how many preventive steps we take. Just look at the colossal 2003 blackout, when 50 million Americans lost power due to a simple error at a power plant in Ohio; or the one a month later, which blacked out 57 million Italians. And these two combined don't even compare to the 2001 outage in India, which affected 226 million people. *The Grid* is the first history of the electrical grid intended for general readers, and it comes at a time when we badly need such a guide. As we get more and more dependent on electricity to perform even the most mundane daily tasks, the grid's inevitable shortcomings will take a toll on populations around the globe. At a moment when energy issues loom large on the nation's agenda and our hunger for electricity grows, *The Grid* is as timely as it is compelling.

ABOUT THE GOVERNMENT-UNIVERSITY-INDUSTRY RESEARCH ROUNDTABLE (GUIRR)

GUIRR's formal mission, revised in 1995, is "to convene senior-most representatives from government, universities, and industry to define and explore critical issues related to the national and global science and technology agenda that are of shared interest; to frame the next critical question stemming from current debate and analysis; and to incubate activities of on-going value to the stakeholders. This forum will be designed to facilitate candid dialogue among participants, to foster self-implementing activities, and, where appropriate, to carry awareness of consequences to the wider public."

The reports listed do not include all National Academies' reports on topics related to the smart grid. To find more on this topic or browse other National Academies reports go to: www.nationalacademies.org.

Government | University | Industry
RESEARCH ROUNDTABLE

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The nation turns to the National Academies—National Academy of Sciences, National Academy of Engineering, Institute of Medicine, and National Research Council—for independent, objective advice on issues that affect people's lives worldwide.