GOVERNMENT-UNIVERSITY-INDUSTRY
RESEARCH ROUNDTABLE (GUIRR)

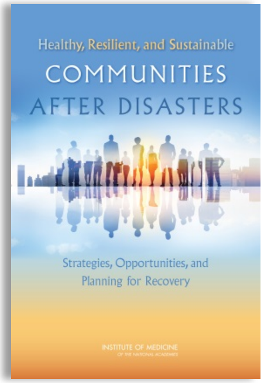
February 23-24, 2016

POLICY AND GLOBAL AFFAIRS

CRITICAL INFRASTRUCTURE SECURITY

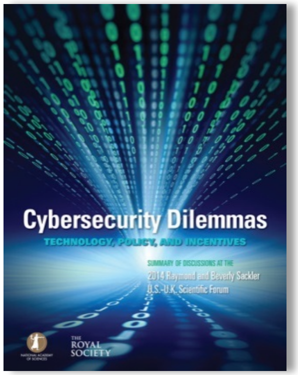
The Role of Public-Private Partnerships

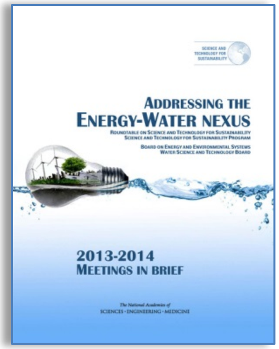
List of selected reports from the Academies related to the meeting topic:
Critical Infrastructure Security



Healthy, Resilient, and Sustainable Communities After Disasters: Strategies, Opportunities, and Planning for Recovery (2015)
In the devastation that follows a major disaster, there is a need for multiple sectors to unite and devote new resources to support the rebuilding of infrastructure, the provision of health and social services, the restoration of care delivery systems, and other critical recovery needs. In some cases, billions of dollars from public, private and charitable sources are invested to help communities recover. National rhetoric often characterizes these efforts as a "return to normal." But for many American communities, pre-disaster conditions are far from optimal. Large segments of the U.S. population suffer from preventable health problems, experience inequitable access to services, and rely on overburdened health systems. A return to pre-event conditions in such cases may be short-sighted given the high costs - both economic and social - of poor health. Instead, it is important to understand that the disaster recovery process offers a series of unique and valuable opportunities to improve on the status quo. Capitalizing on these opportunities can advance the long-term health, resilience, and sustainability of communities - thereby better preparing them for future challenges. *Healthy, Resilient, and Sustainable Communities After Disasters* identifies and recommends recovery practices and novel programs most likely to impact overall community public health and contribute to resiliency for future incidents. This book makes the case that disaster recovery should be guided by a healthy community vision, where health considerations are integrated into all aspects of recovery planning before and after a disaster, and funding streams are leveraged in a coordinated manner and applied to health improvement priorities in order to meet human recovery needs and create healthy built and natural environments. The conceptual framework presented in *Healthy, Resilient, and Sustainable Communities After Disasters* lays the groundwork to achieve this goal and provides operational guidance for multiple sectors involved in community planning and disaster recovery. *Healthy, Resilient, and Sustainable Communities After Disasters* calls for actions at multiple levels to facilitate recovery strategies that optimize community health. With a shared healthy community vision, strategic planning that prioritizes health, and coordinated implementation, disaster recovery can result in a communities that are healthier, more livable places for current and future generations to grow and thrive - communities that are better prepared for future adversities.

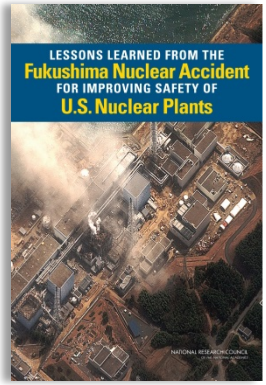
Cybersecurity Dilemmas: Technology, Policy, and Incentives: Summary of Discussions at the 2014 Raymond and Beverly Sackler U.S.-U.K. Scientific Forum (2015)
Individuals, businesses, governments, and society at large have tied their future to information technologies, and activities carried out in cyberspace have become integral to daily life. Yet these activities - many of them drivers of economic development - are under constant attack from vandals, criminals, terrorists, hostile states, and other malevolent actors. In addition, a variety of legitimate actors, including businesses and governments, have an interest in collecting, analyzing, and storing information from and about individuals and organizations, potentially creating security and privacy risks. Cybersecurity is made extremely difficult by the incredible complexity and scale of cyberspace. The challenges to achieving cybersecurity constantly change as technologies advance, new applications of information technologies emerge, and societal norms evolve. In our interconnected world, cyberspace is a key topic that transcends borders and should influence (as well as be influenced by) international relations. As such, both national and international laws will need careful evaluation to help ensure the conviction of cybercriminals, support companies that work internationally, and protect national security. On December 8 and 9, 2014, the Raymond and Beverly Sackler U.S.-U.K. Scientific Forum "Cybersecurity Dilemmas: Technology, Policy, and Incentives" examined a broad range of topics including cybersecurity and international relations, privacy, rational cybersecurity, and accelerating progress in cybersecurity. This report summarizes the presentations and discussions from this forum.

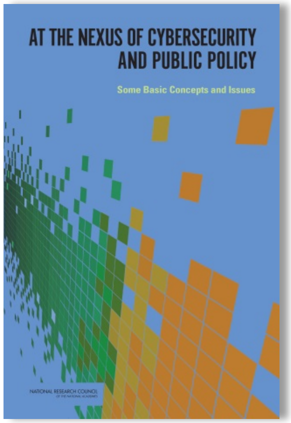

Cybersecurity Dilemmas
TECHNOLOGY, POLICY, AND INCENTIVES
SUMMARY OF DISCUSSIONS AT THE
2014 Raymond and Beverly Sackler
U.S.-U.K. Scientific Forum
THE ROYAL SOCIETY


Addressing the Energy-Water Nexus
2013-2014 Meetings in Brief

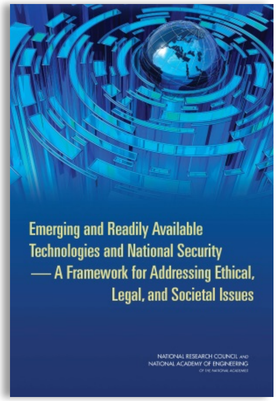
<u>Addressing the Energy-Water Nexus: 2013-2014 Meetings in Brief</u> (2015)
Adequate water and energy are critical to the continued economic security of the United States. The relationship between energy and water is complex, and the scientific community is increasingly recognizing the importance of better understanding the linkages between these two resource domains. Federal agencies, the private sector, and academic researchers have noted that the lack of data on energy-water linkages remains a key limitation to fully characterizing the scope of this issue. Beginning in June 2013, the Roundtable on Science and Technology for Sustainability in collaboration with the Board on Energy and Environmental Systems and the Water Science and Technology Board contributed to the emerging dialogue on the energy-water nexus by holding four related meetings. These meetings were designed to examine emerging technical and policy mechanisms to address energy-water issues. This report summarizes the presentations and discussions from these meetings.

<u>Lessons Learned from the Fukushima Nuclear Accident for Improving Safety of U.S. Nuclear Plants</u> (2014)
The March 11, 2011, Great East Japan Earthquake and tsunami sparked a humanitarian disaster in northeastern Japan. They were responsible for more than 15,900 deaths and 2,600 missing persons as well as physical infrastructure damages exceeding $200 billion. The earthquake and tsunami also initiated a severe nuclear accident at the Fukushima Daiichi Nuclear Power Station. Three of the six reactors at the plant sustained severe core damage and released hydrogen and radioactive materials. Explosion of the released hydrogen damaged three reactor buildings and impeded onsite emergency response efforts. The accident prompted widespread evacuations of local populations, large economic losses, and the eventual shutdown of all nuclear power plants in Japan. *Lessons Learned from the Fukushima Nuclear Accident for Improving Safety and Security of U.S. Nuclear Plants* is a study of the Fukushima Daiichi accident. This report examines the causes of the crisis, the performance of safety systems at the plant, and the responses of its operators following the earthquake and tsunami. The report then considers the lessons that can be learned and their implications for U.S. safety and storage of spent nuclear fuel and high-level waste, commercial nuclear reactor safety and security regulations, and design improvements. *Lessons Learned* makes recommendations to improve plant systems, resources, and operator training to enable effective ad hoc responses to severe accidents. This report's recommendations to incorporate modern risk concepts into safety regulations and improve the nuclear safety culture will help the industry prepare for events that could challenge the design of plant structures and lead to a loss of critical safety functions. In providing a broad-scope, high-level examination of the accident, *Lessons Learned* is meant to complement earlier evaluations by industry and regulators. This in-depth review will be an essential resource for the nuclear power industry, policy makers, and anyone interested in the state of U.S. preparedness and response in the face of crisis situations.




AT THE NEXUS OF CYBERSECURITY AND PUBLIC POLICY
Some Basic Concepts and Issues
NATIONAL RESEARCH COUNCIL

<u>At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues</u> (2014)
We depend on information and information technology (IT) to make many of our day-to-day tasks easier and more convenient. Computers play key roles in transportation, health care, banking, and energy. Businesses use IT for payroll and accounting, inventory and sales, and research and development. Modern military forces use weapons that are increasingly coordinated through computer-based networks. Cybersecurity is vital to protecting all of these functions. Cyberspace is vulnerable to a broad spectrum of hackers, criminals, terrorists, and state actors. Working in cyberspace, these malevolent actors can steal money, intellectual property, or classified information; impersonate law-abiding parties for their own purposes; damage important data; or deny the availability of normally accessible services. Cybersecurity issues arise because of three factors taken together - the presence of malevolent actors in cyberspace, societal reliance on IT for many important functions, and the presence of vulnerabilities in IT systems. What steps can policy makers take to protect our government, businesses, and the public from those would take advantage of system vulnerabilities? *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.

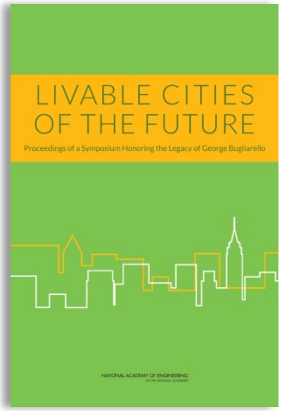

Emerging and Readily Available Technologies and National Security — A Framework for Addressing Ethical, Legal, and Societal Issues
NATIONAL RESEARCH COUNCIL AND NATIONAL ACADEMY OF ENGINEERING OF THE NATIONAL ACADEMIES

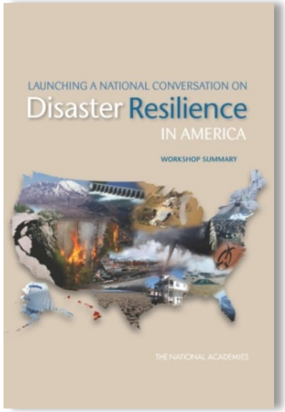
Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal, and Societal Issues (2014)

Emerging and Readily Available Technologies and National Security is a study on the ethical, legal, and societal issues relating to the research on, development of, and use of rapidly changing technologies with low barriers of entry that have potential military application, such as information technologies, synthetic biology, and nanotechnology. The report also considers the ethical issues associated with robotics and autonomous systems, prosthetics and human enhancement, and cyber weapons. These technologies are characterized by readily available knowledge access, technological advancements that can take place in months instead of years, the blurring of lines between basic research and applied research, and a high uncertainty about how the future trajectories of these technologies will evolve and what applications will be possible. *Emerging and Readily Available Technologies and National Security* addresses topics such as the ethics of using autonomous weapons that may be available in the future; the propriety of enhancing the physical or cognitive capabilities of soldiers with drugs or implants or prosthetics; and what limits, if any, should be placed on the nature and extent of economic damage that cyber weapons can cause. This report explores three areas with respect to emerging and rapidly available technologies: the conduct of research; research applications; and unanticipated, unforeseen, or inadvertent ethical, legal, and societal issues. The report articulates a framework for policy makers, institutions, and individual researchers to think about issues as they relate to these technologies of military relevance and makes recommendations for how each of these groups should approach these considerations in its research activities. *Emerging and Readily Available Technologies and National Security* makes an essential contribution to incorporate the full Consideration of ethical, legal, and societal issues in situations where rapid technological change may outpace our ability to foresee consequences.

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

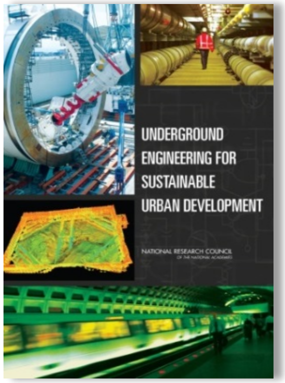
At the beginning of the 20th century an estimated five percent of the world's population lived in cities. Today, half the world's population is urbanized. Urban sustainability is multifaceted and encompasses security, economics, environment and resources, health, and quality of life. It can be viewed as the intersection of two extremely complex and not yet fully understood processes, urbanization and global sustainability, which will increasingly overlap as urban populations continue to grow. Effective policies are critical for addressing urban sustainability, and must be politically realistic in deciding on appropriate balances, such as centralized versus decentralized systems, "soft" versus "hard" solutions, local versus regional focus, agriculture versus pollution, and free markets versus interventions. 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.


LIVABLE CITIES OF THE FUTURE
Proceedings of a Symposium Honoring the Legacy of George Bugliarello
NATIONAL ACADEMY OF ENGINEERING OF THE NATIONAL ACADEMIES



Launching a National Conversation on Disaster Resilience in America: Workshop Summary (2013)

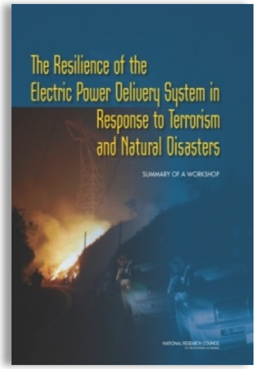
With the increasing frequency of natural and human-induced disasters and the increasing magnitude of their consequences, a clear need exists for governments and communities to become more resilient. The National Research Council's 2012 report Disaster Resilience: A National Imperative addressed the importance of resilience, discussed different challenges and approaches for building resilience, and outlined steps for implementing resilience efforts in communities and within government. Launching a National Conversation on Disaster Resilience in America is a summary of a one-day event in November 2012 to formally launch a national conversation on resilience. Nationally-recognized experts in disaster resilience met to discuss developing a culture of resilience, implementing resilience, and understanding federal perspectives about resilience. This report includes a broad range of perspectives and experiences derived from many types of hazards and disasters in all parts of the country.


UNDERGROUND ENGINEERING FOR SUSTAINABLE URBAN DEVELOPMENT
NATIONAL RESEARCH COUNCIL

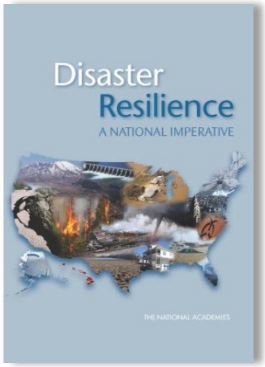
Underground Engineering for Sustainable Urban Development (2013)

For thousands of years, the underground has provided humans refuge, useful resources, physical support for surface structures, and a place for spiritual or artistic expression. More recently, many urban services have been placed underground. Over this time, humans have rarely considered how underground space can contribute to or be engineered to maximize its contribution to the sustainability of society. As human activities begin to change the planet and population struggle to maintain satisfactory standards of living, placing new infrastructure and related facilities underground may be the most successful way to encourage or support the redirection of urban development into sustainable patterns. Well maintained, resilient, and adequately performing underground infrastructure, therefore, becomes an essential part of sustainability, but much remains to be learned about improving the sustainability of underground infrastructure itself. At the request of the National Science Foundation (NSF), the National Research Council (NRC) conducted a study to consider sustainable underground development in the urban environment, to identify research needed to maximize opportunities for using underground space, and to enhance understanding among the public and technical communities of the role of underground engineering in urban sustainability. Underground Engineering for Sustainable Urban Development explains the findings of researchers and practitioners with expertise in geotechnical engineering, underground design and construction, trenchless technologies, risk assessment, visualization techniques for geotechnical applications, sustainable infrastructure development, life cycle assessment, infrastructure policy and planning, and fire prevention, safety and ventilation in the underground. This report is intended to inform a future research track and will be of interest to a broad audience including those in the private and public sectors engaged in urban and facility planning and design, underground construction, and safety and security.

The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters: Summary of a Workshop (2013)

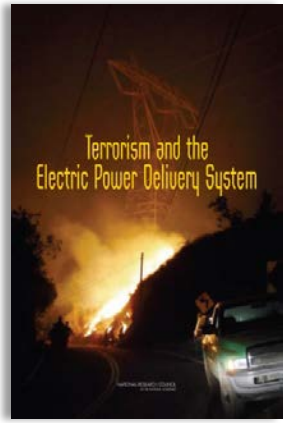

The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters
SUMMARY OF A WORKSHOP
NATIONAL RESEARCH COUNCIL

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. The electric power transmission and distribution system (the grid) is an extraordinarily complex network of wires, transformers, and associated equipment and control software designed to transmit electricity from where it is generated, usually in centralized power plants, to commercial, residential, and industrial users. Because the U.S. infrastructure has become increasingly dependent on electricity, vulnerabilities in the grid have the potential to cascade well beyond whether the lights turn on, impacting among other basic services such as the fueling infrastructure, the economic system, and emergency services. *The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters* discusses physical vulnerabilities and the cybersecurity of the grid, ways in which communities respond to widespread outages and how to minimize these impacts, the grid of tomorrow, and how resilience can be encouraged and built into the grid in the future.



Disaster Resilience: A National Imperative (2012)

No person or place is immune from disasters or disaster-related losses. Infectious disease outbreaks, acts of terrorism, social unrest, or financial disasters in addition to natural hazards can all lead to large-scale consequences for the nation and its communities. Communities and the nation thus face difficult fiscal, social, cultural, and environmental choices about the best ways to ensure basic security and quality of life against hazards, deliberate attacks, and disasters. Beyond the unquantifiable costs of injury and loss of life from disasters, statistics for 2011 alone indicate economic damages from natural disasters in the United States exceeded $55 billion, with 14 events costing more than a billion dollars in damages each. One way to reduce the impacts of disasters on the nation and its communities is to invest in enhancing resilience--the ability to prepare and plan for, absorb, recover from and more successfully adapt to adverse events. *Disaster Resilience: A National Imperative* addresses the broad issue of increasing the nation's resilience to disasters. This book defines "national resilience", describes the state of knowledge about resilience to hazards and disasters, and frames the main issues related to increasing resilience in the United States. It also provide goals, baseline conditions, or performance metrics for national resilience and outlines additional information, data, gaps, and/or obstacles that need to be addressed to increase the nation's resilience to disasters. Additionally, the book's authoring committee makes recommendations about the necessary approaches to elevate national resilience to disasters in the United States. Enhanced resilience allows better anticipation of disasters and better planning to reduce disaster losses-rather than waiting for an event to occur and paying for it afterward. *Disaster Resilience* confronts the topic of how to increase the nation's resilience to disasters through a vision of the characteristics of a resilient nation in the year 2030. Increasing disaster resilience is an imperative that requires the collective will of the nation and its communities. Although disasters will continue to occur, actions that move the nation from reactive approaches to disasters to a proactive stance where communities actively engage in enhancing resilience will reduce many of the broad societal and economic burdens that disasters can cause.

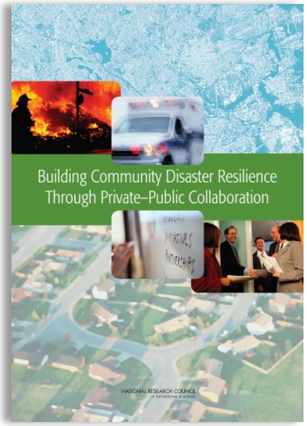


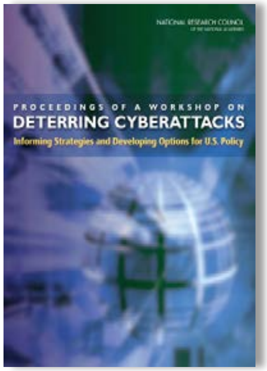
Terrorism and the Electric Power Delivery System (2012)

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. Electric systems are not designed to withstand or quickly recover from damage inflicted simultaneously on multiple components. Such an attack could be carried out by knowledgeable attackers with little risk of detection or interdiction. Further well-planned and coordinated attacks by terrorists could leave the electric power system in a large region of the country at least partially disabled for a very long time. Although there are many examples of terrorist and military attacks on power systems elsewhere in the world, at the time of this study international terrorists have shown limited interest in attacking the U.S. power grid. However, that should not be a basis for complacency. Because all parts of the economy, as well as human health and welfare, depend on electricity, the results could be devastating. 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.

Building Community Disaster Resilience Through Private-Public Collaboration (2011)

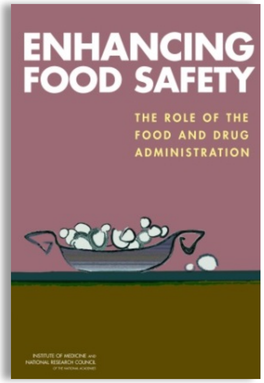
Natural disasters--including hurricanes, earthquakes, volcanic eruptions, and floods--caused more than 220,000 deaths worldwide in the first half of 2010 and wreaked havoc on homes, buildings, and the environment. To withstand and recover from natural and human-caused disasters, it is essential that citizens and communities work together to anticipate threats, limit their effects, and rapidly restore functionality after a crisis. Increasing evidence indicates that collaboration between the private and public sectors could improve the ability of a community to prepare for, respond to, and recover from disasters. Several previous National Research Council reports have identified specific examples of the private and public sectors working cooperatively to reduce the effects of a disaster by implementing building codes, retrofitting buildings, improving community education, or issuing extreme-weather warnings. State and federal governments have acknowledged the importance of collaboration between private and public organizations to develop planning for disaster preparedness and response. Despite growing ad hoc experience across the country, there is currently no comprehensive framework to guide private-public collaboration focused on disaster preparedness, response, and recovery. Building Community Disaster Resilience through Private-Public Collaboration assesses the current state of private-public sector collaboration dedicated to strengthening community resilience, identifies gaps in knowledge and practice, and recommends research that could be targeted for investment. Specifically, the book finds that local-level private-public collaboration is essential to the development of community resilience. Sustainable and effective resilience-focused private-public collaboration is dependent on several basic principles that increase communication among all sectors of the community, incorporate flexibility into collaborative networks, and encourage regular reassessment of collaborative missions, goals, and practices.


Building Community Disaster Resilience
Through Private–Public Collaboration
NATIONAL RESEARCH COUNCIL


NATIONAL RESEARCH COUNCIL
PROCEEDINGS OF A WORKSHOP ON
DETERRING CYBERATTACKS
Informing Strategies and Developing Options for U.S. Policy

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


ENHANCING FOOD SAFETY
THE ROLE OF THE FOOD AND DRUG ADMINISTRATION
INSTITUTE OF MEDICINE AND NATIONAL RESEARCH COUNCIL

Enhancing Food Safety: The Role of the Food and Drug Administration (2010)
Recent outbreaks of illnesses traced to contaminated sprouts and lettuce illustrate the holes that exist in the system for monitoring problems and preventing foodborne diseases. Although it is not solely responsible for ensuring the safety of the nation's food supply, the U.S. Food and Drug Administration (FDA) oversees monitoring and intervention for 80 percent of the food supply. The U.S. Food and Drug Administration's abilities to discover potential threats to food safety and prevent outbreaks of foodborne illness are hampered by impediments to efficient use of its limited resources and a piecemeal approach to gathering and using information on risks. Enhancing Food Safety: The Role of the Food and Drug Administration, a new book from the Institute of Medicine and the National Research Council, responds to a congressional request for recommendations on how to close gaps in FDA's food safety systems. Enhancing Food Safety begins with a brief review of the Food Protection Plan (FPP), FDA's food safety philosophy developed in 2007. The lack of sufficient detail and specific strategies in the FPP renders it ineffectual. The book stresses the need for FPP to evolve and be supported by the type of strategic planning described in these pages. It also explores the development and implementation of a stronger, more effective food safety system built on a risk-based approach to food safety management. Conclusions and recommendations include adopting a risk-based decision-making approach to food safety; creating a data surveillance and research infrastructure; integrating federal, state, and local government food safety programs; enhancing efficiency of inspections; and more. Although food safety is the responsibility of everyone, from producers to consumers, the FDA and other regulatory agencies have an essential role. In many instances, the FDA must carry out this responsibility against a backdrop of multiple stakeholder interests, inadequate resources, and competing priorities. Of interest to the food production industry, consumer advocacy groups, health care professionals, and others, Enhancing Food Safety provides the FDA and Congress with a course of action that will enable the agency to become more efficient and effective in carrying out its food safety mission in a rapidly changing world.

About the Government-University-Industry Research Roundtable (GUIRR)

GUIRR's mission 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. The forum is designed to facilitate candid dialogue among participants, to foster self-implementing activities, and, where appropriate, to carry awareness of consequences to the wider public.

Government | University | Industry
RESEARCH ROUNDTABLE

For more information about GUIRR, visit our web site at
www.nas.edu/guirr
500 Fifth Street, N.W. Washington, D.C. 20001
guirr@nas.edu