# Protecting Our Future

## Shaping Public-Private Cooperation to Secure Criticial Information Infrastructures

Report of a Roundtable of Experts & Policy Makers
Held March 15, 2006 in Washington, DC

By Kenneth Cukier

May 2006

*To order additional copies of this report please contact:*
Viktor Mayer-Schönberger, Roundtable Co-Chair
The John F. Kennedy School of Government
Harvard University
79 JFK Street
Cambridge, MA 02138
Email: Viktor_Mayer-Schoenberger@harvard.edu
For more on the Rueschlikon Conferences please visit http://www.rueschlikon-conference.org


Published in the United States of America in 2006


The March 15, 2006 Roundtable meeting and the publication of this report was made possible through the financial and organizational support of Verizon.

# Contents

Critical information infrastructures (CIIs) — communications or information service whose availability, reliability and resilience are essential to the functioning of a modern economy, security, and other essential social values — have grown significantly in importance. Markets depend on them, as much as government, to function properly.

Even more importantly, CIIs are needed to support the work of other critical infrastructures, from power distribution and water supply to transportation and finance. Yet, CIIs have received comparatively little attention beyond the often-repeated need to protect them from terrorist activity, despite the fact most CII disruptions are caused by natural disasters, poor system design, human error, hackers, or inappropriate public policy.

This report summarizes a roundtable meeting on March 15, 2006 at the National Press Club in Washington DC when leadings experts and policymakers deliberated on the public policy agenda to better protect CIIs. The meeting in Washington followed a similar meeting, the 2006 Rueschlikon Conference on Information Policy in June 2005 in Switzerland.

We thank Kenneth Cukier, the author of this report, for once again penning an excellent and highly readable account of our day-long deliberations. We especially thank Verizon for organizational assistance and financial support in making this roundtable in Washington possible.

Lewis M. Branscomb, *Aetna Professor of Public Policy and Corporate Management, Emeritus*
Viktor Mayer-Schönberger, *Associate Professor of Public Policy*
*Kennedy School of Government, Harvard University*

May 2006

Society depends on critical information infrastructure for everything from phone service and aviation, to cash machines and even power stations. If the networks fail, many other things do as well. But while the importance is understood, the vulnerabilities are not.

Many firms take robust measures to protect their infrastructure from harm by nature, accident or terrorism. However, because networks are interdependent, there is an important need for cooperation and information-sharing that does not always adequately happen, both to prevent problems and restore service after outages occur.

To understand the issue and consider possible approaches to protecting critical information infrastructure, a one-day roundtable was convened that brought together around 30 experts from industry, government and academia. Three major themes emerged:

**1. Fix the Easy Things First:** *The issues are broad and challenging, however before addressing the major obstacles, remedy the more easily identifiable concerns that also must be resolved.*

**2. Design a System:** *Instead of trying to devise an organization to treat every conceivable problem, establish a process so that future, unimagined concerns can be efficiently addressed.*

**3. Harness the Private Sector and Market Forces:** *The entities best placed to protect infrastructure are the owner/operators themselves, provided incentives exist for cross-industry cooperation and information-sharing.*

The report that follows develops these themes in more depth. It explains the interdependence of infrastructure, where vulnerabilities exist and different approaches to overcome them. It notes that new forms of public-private sector cooperation may be needed, yet warns against simply adding bureaucracy. It discusses how market-mechanisms can play a role. Lastly, it identifies possible next steps for industry and government (including basic reforms such as equipping private-sector infrastructure technicians with "emergency responder" IDs for access to restricted areas).

The event was organized by Viktor Mayer-Schönberger and Lewis M. Branscomb of Harvard University's John F. Kennedy School of Government. Looking forward, the participants left with an optimistic belief that protecting critical information infrastructure is possible, helped by the activity of the business sector with the support of government.

## The Business and Politics of Critical Information Infrastructure Protection

The world relies on information infrastructure. Police, hospitals and banks depend on it, as do gas stations and even the electric power grid. If communication networks don't work, many other things we take for granted don't either.

While the role and importance of critical information infrastructure (CII) is often well-understood, its vulnerabilities are less so. And this is usually only apparent when things go wrong and services are jeopardized. So to appreciate just how thorny a problem CII protection is, consider the events of Hurricane Katrina in August and September 2005.

When the storm hit, BellSouth, the regional telecom provider, felt reasonably prepared. It had already activated its emergency plans days before, moved additional infrastructure into place and alerted staff. Much equipment was located on elevated floors or pilings, since the region was a known floodplain. But the problems the company actually encountered were far from the customary concerns of telecommunications.

As electrical lines went down, back-up generators took over — but when the fuel ran dry, new provisions couldn't be driven in. In some cases, government authorities actually confiscated it. In other instances, engineers were forbidden from entering areas for lack of uniform staff IDs to prove they were legitimate phone company employees. Meanwhile, a new problem came from plunderers stealing back-up generators.

Ordinarily, a firm would call the police — but this was not an ordinary time; law enforcement were often unable to help, preoccupied elsewhere. (Ironically, the police faced major troubles themselves because of the very lack of communications.) As a result, BellSouth scrambled to organize private security guards for its staff and equipment, and shared the security service with other firms. But even this posed new problems, such as needing to figure out the law on transporting firearms across state lines. Moreover, vehicles to reach equipment where useless when technicians needed to travel by boat.

What seemed like one problem that could be prepared for — keeping the telecom network running — involved many unexpected ones, involving ID badges, gasoline transport and gun laws. The work of BellSouth was prodi-

gious and services were restored quickly. Yet the lessons from the experience are less complimentary. It shows that even the best plans do not perfectly prepare infrastructure providers to respond. It points to the need for better coordination among different infrastructure players. It underscores the interdependency of disparate services. And it suggests that unless there is a systematic approach to address CII security, the vulnerabilities will fester.

Hurricane Katrina represented the first major test of America's emergency-preparedness and CII protection efforts since 9/11, and in many respects they proved a failure. If there is any cause for optimism, it is this: while the hurricane was an act of nature, much of the problems encountered were the result of human error (e.g., flooding because the levees were breeched; idle generators because fuel supplies were stymied; incompatible communications equipment, etc.). As a result, the protection of CII doesn't need to be left to the gods. It is inherently addressable, so long as people take the initiative to act.

In this spirit, a Roundtable event was organized by Viktor Mayer-Schönberger and Lewis M. Branscomb of Harvard University's John F. Kennedy School of Government, to bring together around 30 experts from industry, academia, and state and federal government (including members of the House and Senate, as well as the FCC Chairman), to consider the problem of securing CII, and to identify possible solutions. The day-long event at the National Press Club in Washington, DC, built upon the discussion and report from the Rueschlikon Conference on Information Policy in June 2005.

This report is intended to continue the momentum. It comprises four brief sections. First, it explains the problem and the limits of conventional approaches. Second, it notes roles for the public and private sectors. Third, it considers how the market system rather than classic regulation can be applied. Finally, it identifies immediate actions that may improve the situation, and suggests possible next steps.

The Roundtable participants offered diverse views, as is natural for any complex issue. Yet there was a consensus that what is most needed is a two-track effort: an emphasis on crises prevention rather than simply reacting to disasters on one hand, and flexible mechanisms to address unforeseen problems when response is called for, on the other hand. Securing critical information

infrastructure is possible, the report concludes, provided the will exists among industry and government.

## 1. Problems and Problematic Remedies

Perfect security does not exist; it is always a matter of tradeoffs. Yet securing critical information infrastructure is made particularly hard because there exist inherent vulnerabilities that cross areas of technology, economics, regulation and culture.

There is a huge interdependence among infrastructure providers. This requires cooperation on prevention (including information-sharing on potential threats and preparations for response), as well as collaboration for the restoration of service after failures occur. While some sectors like telecommunications have long-established mechanisms for sharing information among firms and with government, other sectors do not — nor is there adequate dialogue across different industry sectors. In some instances, a relevant partner may be in a different country.

Nearly all of the infrastructure is owned and operated by the private sector. As a result, federal laws intended to prevent business collusion may actually impede industry cooperation for CII protection. At the same time, rules to prevent government favoritism hamstring agencies from working more closely with the business community on security. And intelligence on security threats presume the recipient is a government employee with a security clearance; new practices would be necessary to share information with the private sector in a way that didn't inadvertently disclose sensitive data.

Meanwhile, competitive pressure on companies actually undermines the resilience of CII. Firms are rewarded for cutting costs, which may come at the expense of security. And as supply chains become more efficient, they lose flexibility that is valuable in times of crises. There are concerns that insufficient economic incentives exist for CII to be protected optimally. Some economists believe CII protection constitutes a market failure, though it is hard to say for sure, considering the very information necessary to determine this is lacking (which critics point to as evidence of the failure).

What is clear is that there is a collective-action problem. "Large companies do not want to invest unless they are assured that their competitors will invest

too," explained Prof. Branscomb of Harvard's Kennedy School. "So there needs to be some sort of industry association to do this, and thus antitrust protection." Alongside this is the perennial question: who pays?

Classic approaches to secure infrastructure are not viable, be it business investment, regulation, technology or simply goodwill. The business community tends to absorb the costs and hope for the best — an approach that is legitimated because the risks are largely unknown, especially across industry sectors. "Security is always too much, until the day it is not enough," said Brian Snow of the National Security Agency, attending and speaking in a personal capacity prior to his retirement from the NSA.

As for regulation, it often lags behind the nature of the problem — driving forward by looking through the rear-view mirror. Regulation also risks shifting the emphasis from true security to legal compliance, and creates a floor rather than identifying a ceiling. Finally, traditional regulation does not allow for the flexibility that CII protection requires. For instance, many participants from industry cited the importance of empowering front-line employees during a crises. But this beneficial autonomy might pose liability concerns if firms had to consider the regulatory ramifications.

At the same time, technology offers no silver bullet — rather, it is always a question of keeping up in an arms race with the problem. Ed Felten of Princeton University posed the pertinent question whether the roughly $100 billion that is spent annually on IT security worldwide is simply keeping pace with the problem, lagging or overtaking it — the nature of the question suggesting that there is no real way to know. Strikingly, technology solutions can actually create a false sense of security. The dark irony of CII protection is that the infrastructure itself can be turned into a weapon, much as airliners were on 9/11.

Yet the biggest obstacle is our mindset: People wanting to secure CII hope to develop plans, when the nature of the problem — the unexpected — by nature cannot be planned for. This is even more true in the case of terrorism, since we must assume terrorists will design their attack to take advantage of perceived weaknesses in CII protection. "The key problem we have today is our culture. Around the world, I see people trapped in old visions," explains Patrick Lagadec of Ecole Polytechnique in France. "It is not a question of ready-made answers to known problems," he says. "We need new answers to new problems — they will not simply descend as gentle rain from heaven."

Since September 11, federal, state and local governments have undergone huge reforms in order to respond to emergency situations, including relying on communications to ensure the survivability of CII. But Hurricane Katrina marks a wake-up call that even these enormous efforts have not produced acceptable results, said Senator Susan Collins, who chairs the Senate Committee on Homeland Security and Governmental Affairs. "We have to face up the fact that this was its first great test — and it failed," she told Roundtable participants, invited guests and the press during lunchtime remarks.

"I am not convinced that we have applied the lessons learned," said Congressman Bennie Thompson in his luncheon remarks. "I know right now that if our communications system went down, we have not put in place the technology for first responders to continue to talk to each another. That is unfortunate, because the technology is there."

## II. The Public and Private Sectors

What is the role of different stakeholders? The best knowledge about how to handle CII protection is with the owners and operators themselves, believes Kevin Martin, the Chairman of the Federal Communications Commission. "I don't think anyone at the Commission thinks we have any more unique insight into what is necessary from a public safety or network reliability standpoint than the infrastructure providers themselves," he said at the start of the Roundtable. Yet he added that the threat of regulation is a useful catalyst to spur industry action — and should that fail, the FCC is unafraid to act.

The ability of the private sector to take precautions and react to emergencies was considered impressive. Companies have elaborate disaster prevention and recovery plans, and are poised to activate them at the first indication of threats. Compared to first-responders in public service, front-line company employees are given greater flexibility to be resourceful, and wider responsibility to make decisions. At the same time, managers elsewhere are able to collect information and assist in the recovery.

For example, in the case of Hurricane Katrina, some companies set up special 800 number lines that employees could call for information, established tent-cities where they and their families could go for shelter and food, and even handed out emergency cash and arranged loans. Wal-Mart allowed

any employee to turn up and work at any store in the region, as they fled the disaster area. Strikingly, Wal-Mart had 66% of its stores in the region back in operation 48 hours after the storm, due to its careful planning and an incredibly efficient — and flexible — logistics system.

These sorts of things hold important lessons for the public sector. "We need to take advantage of that capability and move forward with it," said James Caverly of the US Department of Homeland Security. "We are in this position of having to create this partnership, as we work to evolve the legislative and regulatory frameworks needed to effectively support a true partnership," he added.

Participants from government explained that there is a new shift in perception by the public sector in how they see their role. In the past, attention was focused on the heath, safety and welfare of people, and they did not view their responsibility as assisting economic development. However, Hurricane Katrina and other emergencies have shown that it is through reestablishing a vibrant business community that many disaster-relief goals can be met, and the process of rebuilding communities begun. In other words, to ensure that infants get baby-formula, don't requisition it; instead, help get the supermarkets open.

To do this effectively, government policies need to be more flexible than they are. Rules are important for any bureaucracy to function, noted Jonathan Sallet of the Glover Park Group and a former Department of Commerce official. However, it is also critical to find ways to empower people with as much decision-making discretion as possible, he said. For instance, during Katrina, firms that turned to federal agencies for help were asked whether they had first lodged requests with the municipal and state authorities, and heard back — their policies could not take into account circumstances where there were no longer any functioning government at those levels.

One conclusion is that government should adopt more business-like approaches, such as bypassing extraneous hierarchy during crises, and sharing information. Though people on the ground need to be given the responsibility to make decisions, there needs to be clear leadership from the top. Many participants from industry criticized government for failing to prioritize what elements of CII are truly vital to the operations of government, which infrastructure providers should address first. This, even though a formal priority sequence for restoring downed infrastructure may exist.

It was also acknowledged that government was unprepared and uncoordinated in its response to crises, which impeded the private sector's ability to recover. For instance, the incompatibility of radios used by different emergency responders within the same area or across neighboring districts posed a major problem during Katrina, as it did four years earlier after the attack on the World Trade Center. Indeed, it is some of the most basic functions of the public sector — such as maintaining order, permitting supplies through roadblocks — that government must effectively do in order for industry to do its role.

"Should we just be the people providing the guns to get you where you want to go, or should we have done something prior to that?," asked Christopher Geldart of the Governor's Office of Homeland Security for the state of Maryland, pointing to the need for greater planning and preparation. As one person explained to a Senate committee investigating the problems of Katrina, according to Senator Collins: "Emergency management officials should not be exchanging business cards *during* the crises." That is to say, they should have forged working relationships long before the actual disaster.

Often, cooperation between the public and private sector takes place, but it is not very fruitful, giving rise to a misplaced optimism that CII protection is moving forward, when it is in fact worse-off because this distracts from true security.

For example, some Roundtable participants cited the numerous government-industry committees that exist, to explain how the issue is being addressed. But one participant from industry who interacts with high-level federal committees regarding CII dismissed this. He bluntly stated that the very groups praised as examples of public- and private-sector cooperation were, in fact, "the problem." He continued: "I'm not wasting my time any more doing things for (them), because it is a waste of energy." They request information but do nothing with it; spinning wheels giving the illusion of motion, but without movement.

Others nodded their confirmation of similar sentiments. A few participants explained that there is often better reception at state and local levels, where the issues are closer to home and there is more political will. Meanwhile, the general feeling among participants from government is a healthy recognition that they need to do more, and a better job, of working with the private sector.

There is a gap, or "delta," between what gets done by the public sector and the private sector that could be narrowed for everyone's benefit. "What we've lost sight of is the delta between where my business-continuity plan ends and where the nation's national interests pick up," said Cristin Flynn Goodwin of BellSouth. "And as a result, we have these very, very heavy plans that focus on all threats, all hazards, all risks, all vulnerabilities, when we have the ability to do something with that delta. That's the economic piece; that's the incentive piece; that's where we can turn to the federal government to help us drive, and to prioritize these things — since we now know, as critical infrastructure owner/operators, we have new responsibilities and new roles."

## III. Market Mechanisms for CII Protection

Between the public and the private sector lies the market — it relies on government to function smoothly, but lets industry act in a quick and competitive manner, fueled by the spark of self-interest. Yet the market is not always perfect. In the area of CII, there were questions raised whether left to itself, adequate protection took place.

"There are market-failure characteristics here," noted Eli Noam of Columbia University. "There are externalities that are borne by others, such as by customers that have less information. There is no real liability system in place. There is also the pressure of competition, which leads to a pressure on cost — perfectly legitimately; that is the way the textbooks say it's supposed to be," he explained. "But that also means less slack in the system than there used to be. And so it is totally inevitable that there is an under-investment in security. And nobody is doing anything 'wrong' — everyone behaves perfectly, according to their incentives."

Markets reward good actions and penalize bad behavior. Thus, one approach suggested to enhance CII protection was to adopt market mechanisms as much as possible. In the area of CII, it could be applied in a number of ways.

For instance, industry can form trade associations that specify certain levels of security for the products they procure. By establishing high baseline practices, the intent to purchase at that standard creates incentives for suppliers to meet that standard. At the same time, government can use its market power as a customer in this regard. By cooperating with industry in specifying

standards, government can lower costs for itself and industry by purchasing products that are "commercial, off-the-shelf" rather than ones tailored narrowly to federal requirements (which would otherwise reduce the economies of scale for the products).

Market mechanisms can work in other ways. For example, if government required firms to disclose in some way the steps they take to protect infrastructure, companies would likely be more attentive to what they do, since public scrutiny would be applied. Firms that earned high marks might be seen as more prepared for threats and thus enjoy a higher share price; companies that did not, might be regarded as more of a risk, and its stock price suffer. This was the logic of the US Securities and Exchange Commission when it required public companies in the late 1990s to disclose their preparations on the Year 2000 computer changeover.

Markets play an important role because they aggregate information and signal information. Often, these are price signals, such as the classic supply and demand curve, but the do not have to be simply monetary. Markets a cropping up for everything from reducing environmental pollution to forecasting the probability of future events. Where risk is involved, the introduction of insurance creates a market by rewarding positive actions and punishing bad ones — and therefore effectively changing behaviors. For example, the evolution of fire insurance shifted the emphasis from fire brigades to fire prevention (in the form of building codes, identification of flammable materials, etc.). It marked a significant transformation in how large-scale social concerns could be addressed.

But in order for markets to act they need information, which today is lacking, as are incentives to share data and the trusted intermediaries to aggregate it. "It is a very complex, temporal and elusive goal to say 'we are going to secure our nation's infrastructure'. A risk-management approach is obviously much better, [because] it allows you to moderate, or at least modulate, how much you put against respective threats against the baseline," noted Robert Liscouski of Content Analyst, who formerly served as an assistant secretary at the Department of Homeland Security.

The idea of creating a market for CII security represents a novel approach, between classic regulation on one side and the private sector's know-how on the other. "The new thinking is in fact, we don't want to have an organiza-

tion any more. We already have too many organizations, too many boxes," explained Prof. Mayer-Schönberger of Harvard's Kennedy School. "Instead of a new organization that is a mechanism of coordination, what we suggest here is to use another mechanism that is very tried and works — namely, the market. Can we utilize the market rather than an organization? Can we use competition rather than coordination?," he asked.

Of course, market mechanisms get applied even if there is no formal attempt to establish them. Frank Cilluffo of George Washington University and a former White House official on homeland security, noted in his dinner remarks the evening preceding the Roundtable that if security experts do not define what is best, the trial lawyers will. That is another form of market mechanism, but one based only on costs, not rewards.

Markets are predictive. They parse information not just for the immediate situation, but with an eye towards the future. They don't presume to know answers, but are designed to inform decisions so novel answers can emerge. Markets are inherently ever-changing because circumstances are. In the face of unpredictable calamities and imperfect preparation and responses, the question is raised whether markets or government produce better overall results. So far, the evidence seems to favor markets, but doubtless added strength comes from a mix of the two.

This is not to say that the private-sector and market approaches are necessarily the best way forward. Some participants recoiled at the idea of throwing the issue to helter-skelter forces, where *laissez-faire* (hands-off) may end up as *laissez-tomber* (let it drop). And there were concerns that replacing regulations imposed by government with rules dictated by market-institutions was similarly problematic, since the infrastructure owners and operators themselves may be better-placed to understand and address the problems. Indeed, there are many ways to attain CII protection; markets in their myriad forms are but one.

## IV. Immediate Actions to Consider

Faced with the enormity of CII security, it is easy to feel paralyzed. Moreover, the very act of addressing some issues means others are left for later. As Ms. Goodwin of BellSouth put it: "We have more plans than we know what to

do with. We need prioritization. By looking at all hazards, we are not attacking the most critical ones." So how to make such judgments? The approach suggested by many participants was to tackle the relative easy areas first, and momentarily defer the more complex concerns. Thus, before building an ocean-liner, plug the holes in the dinghy — it's far better than sinking if it rains.

There are a number of things industry can do. First, CII owners and operators should look not just at "best practices" but "baseline practices." These, says Sam Horowitz of Hewlett Packard, are practices that "if you don't do it, you're liable, and if you do just this, you're probably liable, too." It doesn't presume to be a ceiling whatsoever, but at least demarcates the floor. Just the introduction of such a concept would require firms to perform due diligence on their CII protection practices, a good thing in itself.

Second, companies need to develop internal strategies for responding to crises, even if the optimal solution would be to find ways to prevent them in the first place. It is essential that employees are able to self-organize into collaborative, creative teams that can handle numerous unexpected crises at once. "We are going to constantly strengthen the physical networks, the economics networks — but what about the human networks… to mobilize, organize and make decisions?," asks Kathryn Brown of Verizon. "Here's the lesson of Katrina: Those teams needed to have roots prior to the crises," she says. "There has to be relationship-building all along the way that prepares us for the moment when we need to trust each other. The actual thing that must be done may or may not be known… But we already have a team together that knows how to start thinking about it."

To do this effectively, firms will need to forge relationships across other companies in the sector and other industries, though organizing this cooperation represents the more complex activities to be treated once the immediate concerns are addressed. As a first step, participants suggested that firms do practical scenario-planning, with an eye for establishing ways in which employees can exercise discretion and resourcefulness for changing situations. Plans and drills are not sufficient — but they are necessary.

Government has important practical first steps, too. Many participants cited the need for the public sector to restore and maintain basic order in times of crises, such as providing security protection to CII engineers making repairs, escorting fuel convoys, etc. What is impermissible are actions dia-

metrically opposed to this, such as confiscating fuel without authorization. It places the onus on government to reassess and reform its response policies for emergencies, an issue that officials acknowledged needed to happen.

Building on this, government needs to support the actions of CII operators to maintain or repair their systems. One simple but significant step to improve coordination would be to designate certain private-sector infrastructure technicians as "emergency responders" and equip them with official identification badges. This would help ensure that engineers have smooth access to restricted areas during times of crises in order to repair critical infrastructure.

At the same time, there is the need for more thoughtful governmental policies to permit greater flexibility by officials in times of crises. One important reform singled out by participants from both industry and government was enabling governors to temporarily suspend certain local laws in times of emergency (and possibly at the federal level too). This is so that regulations that are reasonable at normal times — such as covering zoning, environmental protection, etc. — do not hamper relief efforts during a crisis. A small statutory modification such as this could lead to vastly improved disaster response.

Some actions require the efforts of both government and industry. Interoperability for communications devices among first-responders is imperative, and can only occur by the joint work of the technology industry and government. In many respects, the technology already exists — the technical standards are set, and different radio spectrum allocations need not be a limiting factor. The problem has largely been one of the diverse procurement policies of the over 60,000 local authorities in the United States that are customers of these products. Since 9/11, the federal government earmarked for states and localities over $1 billion to remedy this issue, but still it persists. This was roundly considered inexcusable, and a problem to overcome immediately.

A second area where the public and private sector can come together is in bringing parties to the table to forge deeper cooperation. Rick Murray of Swiss Re noted the need for a "dramatic mobilizer" to serve as a lead convener for discussions, or the momentum may stall due to a chicken-and-egg problem. To facilitate this sort of activity, government can provide antitrust immunity so firms can more easily share information and cooperate in other ways.

Looking further ahead, a consensus among participants was that some form of partnership between government and industry was useful for CII

protection, but should avoid creating new bureaucracy that impedes action. For instance, regulators could resist creating check-list standards, but approve industry practices that if implemented, could reduce a firm's liability from negligence in case of CII failures. Most importantly, securing CII is a "complex science" that requires the expertise of many disciplines rather than any single group, explained David Farber of Carnegie Mellon University, who served as the FCC's chief technologist in 2000-01.

## Conclusion

Critical information infrastructure protection appears to be an intractable problem, but this is not so. It only seems this way, because it is timeless problem. As David Clark of MIT pointed out, a 1991 report from the US National Academies' Computer Science and Telecommunications Board called "Computers at Risk: Safe Computing in the Information Age," which he chaired, offered many of the same recommendations that were bandied about the Roundtable: "best practices"; "information sharing"; "more R&D"; and an "organizational institution" to carry the work forward.

Yet the parallel Dr. Clark raises should not bring despair but highlight that the effort must remain ongoing. In the 1990s, computer security *did* improve; export restrictions on encryption technology *were* lifted. To be sure, security breeches increased enormously, as hackers, viruses and natural disasters threatened infrastructure. But the ability of these systems to remain operational improved tremendously over that time, too.

Moreover, though CII security constitutes a timeless concern, the new thinking by Roundtable participants is to not simply create a new organization to tackle the matter, but to bring to bear the system of the market to generate incentives, both positive and negative, to address the issue. "Don't persist in thinking this is a security problem," says Dr. Clark, "these are social questions." Or, as Prof. Noam of Columbia University put it: "This is not a technical issue — it is an informational issue."

The Roundtable discussion coalesced on a number of areas of rough consensus:

• **Design a process, not solve a problem:** *Preparing for specific sorts of crises is misguided; it is imperative to establish a mechanism to deal with unknown, multiple crises at once.*

• **Fix the easy things first:** *Deal with the complex issues once the basic problems are addressed. If everything is a priority, nothing is.*

• **Harness the power of the private sector:** *The business community has inherent incentives to protect and restore CII; government should encourage this activity, support it in crises, and adopt lessons from it.*

• **Use market forces:** *Marketplace mechanisms offer enduring ways to create incentives for positive behaviors (be it building products or taking precautions) while punishing riskier actions.*

• **Focus on prevention, not just response:** *Taking steps to minimize the likelihood of CII failures, rather than simply recovering from outages, is vital and requires a shift in mindset.*

• **Build new collaborations, not new institutions:** *CII security requires working with partners within and across industries, as well as between the public and private sector, while minimizing bureaucracy.*

One participant posed a challenge to the Roundtable — a thought-experiment: What would have needed to happen before Katrina struck, so that what turned out to be a major problem, was actually never encountered? For instance, if back-up generators were flooded, what would have induced the equipment to have been placed higher in the first place? If police radios failed because batteries couldn't be recharged, what would have naturally led authorities to stockpile fully-charged extras?

The question is essential, because it strikes at the heart of the problem: critical information infrastructure protection requires a living, breathing, adaptable system of response to a changing threat environment, technical landscape and regulatory atmosphere. Trying to address the matter in a centralized manner by experts or committees is bound to fail, for it can never account for all eventualities. Indeed, some participants dismissed this approach as a modern-day "Gosplan," referring to the group that devised the Soviet Union's five-year economic plans.

The implications of the thought-experiment is that the best way for CII protection to move forward is not by any seemingly wise answers — be them corporate policies or government regulation — but from the decentralized decision-making of individual entities, based on their needs, and fueled by the right incentives. To spur the self-interest necessary so that beneficial decisions

are made — elevating fuel-tanks; stockpiling batteries — a useful approach is to reward or punish certain behaviors.

Regulations can do this, as can industry, acting through what it knows best: the market. The choice of which to adhere to is up to business and government to decide. The only option that is unrealistic is inaction.

## About the Author

**Kenneth Neil Cukier** covers technology and regulation for *The Economist* in London. He was a research fellow at the National Center for Digital Government at Harvard University's John F. Kennedy School of Government from 2002 to 2004, and serves as the rapporteur for the Rueschlikon Conference on Information Policy.

## Roundtable Participants

**David Barron** *AVP National Security, Federal Relations, BellSouth*

**Ann Beauchesne** *Executive Director of Homeland Security, U.S. Chamber of Commerce*

**Mark Bradley** *Program Analyst, Critical Infrastructure Protection Portfolio, U.S. Department of Homeland Security*

**Paul Chandler** *Member, Homeland Security Dialogue Forum and Vice President, Communications, Washington Resource Associates*

**Susan M. Collins** *United States Senator (R-ME)*

**Thomas J. Donohue** *President and CEO, U.S. Chamber of Commerce*

**Paul Domich** *Director, Critical Infrastructure Protection Portfolio, U.S. Department of Homeland Security*

**Christopher Geldart** *Assistant Director, Governor's Office of Homeland Security, Maryland*

**Miriam Heller** *Office of CyberInfrastructure, National Science Foundation*

**Jake Olcott** *Staffer, U.S. House of Representatives Committee on Homeland Security*

**Lewis Branscomb** *Professor Emeritus, Kennedy School of Government, Harvard University*

**Kathryn Brown** *Senior Vice President for Public Policy Development, Verizon Corporation*

**David Clark** *Senior Research Scientist, MIT Laboratory for Computer Science*

**Kenneth Cukier** *Technology Correspondent, The Economist*

**David Farber** *Professor, Carnegie-Mellon University*

**Ed Felten** *Professor, Princeton University*

**Cristin Flynn Goodwin** *Director, Homeland Security & Strategic Policy, BellSouth*

**Sam Horowitz** *Director, IT Security Strategy and Architecture, Hewlett-Packard*

**Patrick Lagadec** *Director of Research, Ecole Polytechnique*

**Robert Liscouski** *CEO, Content Analysts; Former Assistant Secretary, Infrastructure Protection, U.S. Department of Homeland Security*

**Kevin Martin** *Chairman, Federal Communications Commission*

**Viktor Mayer-Schönberger** *Associate Professor, Kennedy School of Government, Harvard University*

**Richard Murray** *Chief Claims Strategist, Swiss Re*

**Eli Noam** *Professor and Director, Columbia Institute for Tele-Information, Columbia University*

**Jonathan Sallet** *Partner, The Glover Park Group*

**Brian Snow** *Security Expert*

**Bennie Thompson** *United States Congressman (D-MS)*

Note: Affiliations are listed for identification purposes only.