Infrastrucutre” is defined as “the basic facilities, services, and installations needed for the functioning of a community or society, such as transportation and communications systems, water and power lines, and public institutions.” Societies invest in infrastructure to meet their current and future needs and thus infrastructure reflects the evolution of technology from simpler to more complex, and, in many parts of the world, increases efficiency for its operators, allows greater safety for society as a whole, and offers greater consumer choice.

Diminishing infrastructure moves the society it supports toward less comfort and safety, from plenty to scarcity, from richness to want. Societies recognize their critical dependence on these “commons” and adopt policies and processes to distribute infrastructure and services and to protect them from damage and misuse. Conversely, attacking a society implies threatening its people and infrastructure systems. Denial of access to such basics as water, energy, and transit is a form of international conflict that threatens a nation’s security and often leads to war.

The industrial revolution greatly increased the extent and complexity of the world’s infrastructure, its connectivity, and its technical and economic interdependencies. Developed nations have, over the past generation, entered a second, equally significant, period—that of the information revolution. Information technology (IT) penetrates into many aspects of life for an increasing number of people throughout the world, enriching us but also producing systems of such complexity that they create new dependencies and risks to society.

**Attacking Infrastructure**

Since World War II there have been two primary ways in which...
attacks on infrastructure proceed: aerial bombardment and economic sanctions by nation-states. Both require substantial resources, the former in military capacity, the latter in political and economic strength.

Concerns about the integrity of modern IT-based infrastructure systems go beyond the two primary traditional threats, because even limited failures in extensive and interconnected systems can cause widespread disruption and damage. In addition to hostile nation-states, international and domestic terrorism and organized crime have the demonstrated potential to undermine societies and diminish confidence in the ability of social and political structures to fulfill their expected roles. These emerging concerns over the vulnerabilities of modern infrastructures have been highlighted by the President’s Commission on Critical Infrastructure Protection (PCCIP) in the U.S. and a similar group under the Ministry of International Trade and Industry (MITI) in Japan [1, 5].

The industrial revolution had as a basis mechanical and electromagnetic technologies in the generation and control of power and transportation. But the control of such systems remained largely mechanical, and always with manual back-up. The information revolution has expanded the sophistication of control systems. Sensing of system status, signal processing, hardware and software control logic, system optimization, and fault diagnosis are heavily automated. Operators are remote from the systems they control. Systems do not always behave as their designers intended, nor is their essential software necessarily understood in all its details. As control facilities are interconnected to increase capital and labor productivity, as already complex systems become linked to other complex systems to produce ever more intricate structures, and as rapidly developing IT drives changes that defy effective configuration management, control inevitably slips away. Failure modes and the consequences of failure can not be foreseen.

Infrastructure systems are tested daily by accidents, natural disasters, and human error, and thus engineers and managers have substantial opportunity to harden their systems, learn from errors, and prepare for future stresses. Were this the only concern, societies might take comfort in relying on professional and economic drivers for greater infrastructure safety and reliability.

But, infrastructure systems face not only the random processes of failure and error, they also can be maliciously attacked through the very devices that otherwise enhance their operation. Centralized architectures provide opportunities to disable the heart of a system, inducing disruption over large operating areas. Decentralized architectures provide vulnerable points of entry at the periphery. In both cases, what happens at the interfaces between the large numbers and types of computers, operating systems, control software, and communication systems can be exploited by an attacker. Exacerbating the problem of cyber attacks is the global availability of penetration tools and information on their use, and a deficient sense of responsibility among many computer-literate people who view information systems as fair game and fun to penetrate.

But are these hypothesized threats real? Are they more serious than the other risks societies and individuals already necessarily assume?

There are two types of answers to these questions. The first, empirical in nature, is that malicious attacks on infrastructures are taking place as you read this. In national security terms, so far they have been “low level,” but they impose costs on society. These are attacks by white-collar criminals, by disgruntled employees and ex-employees, and...
by hackers. They have increased the level of activity in the security industry, and added the need for cyber security to that of physical security. They are increasing the market for insurance products to protect against loss, including extensive self-insurance, by operators of such as the banking and finance and transportation infrastructures. So attacks are indeed real, and they can be quantified, at least to the extent that they are detected and reported. They involve theft of service, theft of information, reduced integrity of data, and invasions of privacy.

The second type of answer is to anticipate that worst-case scenarios of widespread attacks on national and international infrastructures by state-supported adversaries, the high level national security threats, will eventually happen if we allow them to. In this sense, the PCCIP’s report may be viewed as a call for prudent actions, lest these concerns eventually be demonstrated to have been accurate.

Protecting Infrastructure
What, then, are these prudent actions? Some of them are of a “terminal defense” nature, undertaken by owners and operators, to protect the individual nodes in a network. These include hardening nodes against physical and electromagnetic attack, erecting firewalls, backing up operational information, providing redundant capacity, and other “best practices.” Relying solely on such measures, however, ignores Sun Tzu’s admonition that a passive defense is futile.

The total system is greater than the sum of its nodes. Focus on the system aspects of protection calls for collective actions, such as undertaking audits of system operation and exchanging the information with other operators to facilitate detecting patterns of distributed attacks, providing redundant system capacity, preparing to reallocate a system load if attacked, preparing plans to ration diminished system capacity, and assisting system reconstitution. But even more important than these largely post-attack measures are those intended to prevent attack. Among these are steps to deter attacks, to take cooperative measures within the infrastructure industry to promote improving the state of the art in system security, and to exchange threat information so that operators can make investments commensurate with the risks they face.

The thrust of the present discussion is on the domain of collective action, especially on collective international actions to diminish the likelihood and consequences of cyber attacks on infrastructure.

A question to be addressed, therefore, is what are the bounds of infrastructure systems and what organizations are critical for collective action? The bounds of an infrastructure system naturally depend on the specifics of each system. The charter of the PCCIP identified eight: telecommunications, electrical power systems; gas and oil transportation and storage; banking and finance; transportation, water supply systems; emergency services (including medical, police, fire, and rescue); and government services [2]. These vary greatly in the extent of their connectivity and on the relationship of each to political and legal jurisdictions.

In many countries, some infrastructures, like water supply, can be local, or within or among first-tier domestic political jurisdictions like states or provinces. Emergency services are provided at the local or provincial level, although there can be a need for international coordination as in the case of disasters near the boundaries of different jurisdictions. Others, such as transportation, tend to be organized at state or national levels, although important aspects of air and marine transport are international in character. But many infrastructures are inherently international—telecommunications, electrical power, gas and oil transportation and storage, and banking and finance. Thus, dealing with their protection is a matter of international organization and cooperation.

Infrastructure interdependencies are a particularly important element of the issue, because they are unlikely to be a primary attention of the system operators. Such interdependencies are critical for two of the identified infrastructures: telecommunications and electric power. Not only do they depend on each other—telecommunications equipment requires electrical power and electrical power system operation depends on distributed control facilities—but most other infrastructures rely on both. For these reasons the substance of international attention must start with telecommunications and electric power. Of these two, the electric power system interdependencies...
are usually between adjacent jurisdictions, while those for telecommunications derive from their global extent.

**The Need For Collective Action**

As the PCCIP stated:

“… protecting our infrastructures at home is not enough. Many aspects of infrastructure operations extend beyond our national borders, and even beyond the control of their owners and operators. The very nature of the cyber dimension renders national borders almost obsolete, and national laws and policies based on those borders of less and less consequence.”

There are other reasons besides the multinational connectivity of what are essentially shared infrastructure systems for addressing protection in terms of collective actions among sovereign countries. Several have been noted earlier: facilitating the exchange of information regarding security measures and threats; and facilitating agreements to provide redundant capacity, to share load, and to assist in reconstitution. These are relatively straightforward and may, in some cases, be implemented under existing international treaties and administrative agreements.

One possible action that is more complex, however, is to construct an international order that will deter cyber attackers. Deterrence rests on the paradigm of detect-locate-identify-punish, and to do so with sufficient certainty that cyber attacks on infrastructure will not escape the prospect of legal action or international sanctions against the attacker. Detection of system attacks requires international cooperation in pooling system “anomaly” data if evidence of coordinated attacks, or their precursor probes, is to be available for analysis and for use in formulating responses. Location requires backtracking attacks from target to source, recognizing that routing attacks through multiple locations and nations serves to conceal the points of origin. Identification requires the cooperation of local authorities to pursue their citizens, or to impinge on their sovereign authority to investigate and punish. Punishment itself has two faces. One is a law-enforcement face, where civil or criminal statutes are violated. This then defines the character of the punishment. The other is a national or international security face, where a relationship between the specific attack and a sponsoring sovereign state must be established.

Finally, the greater the degree of economic development in a country, the more that country stands to lose through a cyber attack. The inevitable spread of IT will have the effect of putting more nations at greater risk over time. Thus the time is appropriate to take international action to reduce the likelihood that cyber attacks will be seen as an effective threat to international development and order. The leading nations of the world need to exercise global leadership in understanding and controlling the adverse consequences of the technologies on which we all depend.

**Obstacles to Collective Action**

The principle of sovereignty and the diversity of the international system of sovereign states may impede cooperation in enhancing cyber security. A discussion of information attacks from the standpoint of existing concepts of international law is provided in [3], where it is noted that the absence of prohibitions against information warfare is significant because the general rule is that whatever is not prohibited is permitted. This lacuna prevents the direct application of much of the body of existing treaties and agreements to support collective international action against cyber attacks.

Nevertheless, we adopt the view that cyber attacks are, or should be, *illegal* acts subject to investigation and prosecution by national law enforcement agencies acting within a context of international legal agreements. However, it must be recognized that a sovereign state exerts exclusive jurisdiction over actions within its territory, and that gov-
ernments have no independent obligation to cooperate with one another [4]. Furthermore, even when international or bilateral treaties for mutual legal assistance between law enforcement agencies exist, they generally contain exceptions that permit the parties to refuse cooperation under certain circumstances such as to protect sovereignty, security, or similar overriding interests.

At the punishment end of criminal law enforcement, further complication derives from the fact that virtually all extradition treaties contain a “double criminality” requirement mandating that an extradition request be based on an offense considered illegal under the laws of both the requesting country and the one to which the request is directed.

Considering the relatively recent emergence of cyber threats, the varying degrees of appreciation of the threat among the nations of the world, and the absence of common legal structures defining criminal actions, collective international action against cyber criminals is problematic at best. The U.S. has already faced this difficulty at least twice. During the Persian Gulf War, Dutch hackers who attacked Pentagon computers were beyond the reach of U.S. justice because the Netherlands did not recognize their activities as crimes. And in 1995, an Argentine hacker who broke into sensitive U.S. systems avoided punishment because his country had insufficient computer crime legislation.

The pursuit of infrastructure assurance through liability allocation faces similar obstacles. Liability rules vary between and within countries. Furthermore, a court may not be able to obtain civil jurisdiction over the entity that an injured party may wish to hold liable, particularly as extradition does not apply to civil matters.

Administrative arrangements to achieve infrastructure protection will be complicated by the number and types of organizations involved. At the national level, reaching agreement requires that all parties understand the issues with a similar sense of urgency before they will put it on their agendas. Even if some nations, most likely the most developed, do agree on the importance of joint action, differing domestic priorities may intervene. Technical standards for system security and safety provide one promising avenue for cooperation, though standards may be seen as an attempt to establish or maintain control of markets as, for example, current debates over the allocation of top-level domain names are seen as attempts by the U.S. or Europe to exert control over Internet commerce.

The uneven status of privatization and deregulation in telecommunications means countries have varying mixes of public and private actors in their decision-making processes. Where one country’s PTT official may decide, another country may rely on executives at several companies, possibly operating under a national regulatory structure.

Differing national concepts of freedom and privacy may also hinder coordinated efforts. National laws and practices differ on such matters as bank secrecy or the necessity to protect personal data. Some governments may be more concerned with regulating communications content for political or religious reasons than with protecting the communications networks themselves.

**Moving Forward**

Obstacles to one are challenges to another, and opportunities to yet another. Thus the preceding is more in the nature of initial and boundary conditions than as prohibitions. There seem to be three axes along which progress is needed. The first is to raise the level of consciousness of the issue of infrastructure protection, to place it on the agendas of more developed countries, and to alert developing countries to the possibility that unwise technical and legal “system architectures” can be limiting their potential.

The second is to encourage an understanding of national responsibilities in the matter of infrastructure assurance and protection to international players who share dependencies. To this end, attempts to standardize the criminality of computer intrusions for purposes of investigation and extradition of perpetrators will be helpful.

The third is to lay foundations in international law that will be required to achieve effective cooperation between companies, agencies, and nations. Where and how might such efforts be accomplished? There are a number of organizations that could play a role in furthering an international agenda.

For example, the International Telecommunications Union (ITU) sets standards for telecommunications equipment and coordinates national efforts to avoid broadcast interference. A significant characteristic of the ITU is that although its members are
nation-states, various companies acting as members of national delegations participate in drafting technical proposals and participate in working groups. It may, therefore, provide a forum for pursuing telecommunications infrastructure protection.

Another institution, the International Civil Aviation Organization, has succeeded in coordinating and harmonizing national aviation policies. This case is particularly interesting because coordinated international action, as illustrated by the Montreal Convention on the Suppression of Unlawful Acts Against Civil Aviation, has successfully guided responses to international terrorism directed against airlines. The signatory nations agreed to recognize attacks against civil aircraft or air navigation facilities as illegal acts and to extradite or try suspected offenders.

Other organizations that can serve as role models or provide direct assistance in enhancing infrastructure protection are Interpol, which promotes international criminal investigation assistance and information sharing; the United Nations; Intelsat; the World Trade Organization; and the Organization for Economic Cooperation and Development, which has already issued guidelines for the security of information systems. Canada, France, Germany, Great Britain, Italy, Japan, Russia, and the U.S. are trying to address some of these difficulties. Last December their justice ministers issued a communiqué calling for improved cooperation in investigations, harmonization of computer crime legislation, and better procedures for sharing information and evidence.

Reaching international or bilateral agreements, even when appropriate forums exist, is a lengthy process requiring actions within each potential signatory country, and meetings whose only purpose is to agree to meet at some later time to consider the issue, to establish an appropriate process, and to frame the agenda. Such efforts, in turn, require responsible technical communities within each country able to inform debate and assist in analyzing and drafting national positions. It is to one such community that this discussion is addressed.

References

Readers are encouraged to send comments, suggestions, anecdotes, insightful speculation, raw data, and submissions of articles on subjects relating to international aspects of IT to: Sy Goodman, CISAC. 320 Galvez, Stanford University, Stanford, CA 94305-6165 or sgoodman@leland.stanford.edu; fax: (650)-723-0089.

Stephen Lukasik (stephen.j.lukasik@cpmx.saic.com), was Director of ARPA, Chief Scientist of the FCC, and a Vice President of Xerox, TRW, and Northrop. Lawrence Greenberg (LawrenceG@fool.com) is General Counsel for The Motley Fool, Inc. Seymour Goodman is Director of the Project on IT and International Security, Stanford University.

© 1998 ACM 0002-0782/98/0600 $5.00