

REGULATING THE INTERNET

Report to the
President's Commission
on Critical Infrastructure Protection

1997



This report was prepared for the President's Commission on Critical Infrastructure Protection, and informed its deliberations and recommendations. The report represents the opinions and conclusions solely of its author, Ethan B. Kapstein, Ph.D.

Ethan B. Kapstein, Ph.D

Ethan B. Kapstein is the Stassen Professor of International Peace at the Humphrey Institute of Public Affairs, University of Minnesota, where he teaches courses in the areas of comparative and international economic policy. Previously he was Vice President of the Council on Foreign Relations, and a Principal Administrator at the Organization for Economic Cooperation and Development. From 1984-1994 he was at Harvard's Center for International Affairs in a variety of positions, including as Director of the Economics and National Security Program. Kapstein has served as an intelligence officer in the U.S. Naval Reserve, and worked for four years as an international banker. He is the author of numerous books and professional and policy articles, including *Governing the Global Economy. International Finance and the State* (Harvard University Press, 1994) and "Workers and the World Economy," *Foreign Affairs* (May/June 1996). He received the A.B. from Brown University, and the Ph.D. from the Fletcher School of Law and Diplomacy. He is a member of the Council on Foreign Relations and the International Institute of Strategic Studies.

TABLE OF CONTENTS

Executive Summary	1
Report	
1. Introduction: National Security and the Global Economy	5
2. Modes of Regulation	9
3. The Global Information Infrastructure	17
4. Regulating the Internet	21
a. Non-Governmental Regulation	25
b. Attempted International Cooperation: Encryption Policy	29
5. Conclusions and Policy Recommendations	42
Notes	46

EXECUTIVE SUMMARY

The global economy has always challenged national security officials. Today, the challenges are even greater, not only because of the rapid evolution of information technology and the associated growth in transactions and communications, but also because the end of the Cold War has raised important questions about the appropriate sphere of government activity. Areas that were once almost exclusively reserved to the government--for example, encryption policy--are now at the heart of the internet's future economic development. It is in this complex and changing context that regulatory policy for the internet is being shaped.

This report provides an overview of regulatory approaches now being taken with respect to the net. It contrasts the informal, non-governmental approach taken to date with respect to internet technical standards, with the formal, governmental-directed policy on encryption. Accordingly, the report characterizes the internet as having a "mixed" regulatory environment with both governmental and non-governmental actors providing important regulatory services. Further, the purview of these services is national, international, and supranational.

Perhaps the best developed area of regulatory cooperation is technical standards. These standards are largely promulgated by an informal body, the Internet Engineering Task Force (IETF) which has something close to "supranational" powers. That is, members of the IETF do not represent national governments or national interests. Instead, they are scientists and engineer—some from government, but others from universities and the private sector--who seek the "best" technical solutions to the problems that face them at the moment.

The least developed area of regulatory provision, in contrast, is probably formal international cooperation undertaken by governments, with encryption policy providing a case in point. This is puzzling, since one would expect states to respond to the “borderless” internet by creating a dense web of multilateral agreements. Further, encryption is an issue that sits close to national security, so we would expect the government to play an active and authoritative role in policy development and execution. Yet a deeper examination uncovers why international cooperation has been elusive.

First, in many respects the internet is not yet “ripe” for formal international agreements. In order for an issue-area to be ripe for a regulatory response, three factors must be present: an authoritative definition of what the problem is; an appropriate and proportionate solution to the problem; and a body capable of enforcing the solution. With respect to international regulation of the internet, states continue to have important differences with respect to such issues as encryption policy or content legislation, and indeed the intensity of internet usage varies widely across countries. This means that countries do not yet share a common vision of what the “problem” is, much less what the appropriate solutions are. Further, no international body has independent enforcement powers.

Second, and paradoxically, to the extent that the internet is truly borderless, countries may be expected to look mainly to themselves, rather than to some international or supranational agency, to suppress criminal activity. This is because, in the absence of international bodies with strong enforcement powers, states are the only actors with the authority to prosecute criminal behavior.

That means that any international regime for the internet must rest on the foundation of *home country control*. To the extent that states are able to define what constitutes criminal activity on the net, they will strike international agreements. But these agreements will only be effective to the extent that governments are able to track-down and prosecute criminals within their borders. This “formula” of international cooperation based on home country control is, in fact, found in many other issue-areas associated with globalization, from pollution control to telecommunications to international finance.

This “mixed” model of internet regulation, with both governmental and non-governmental actors playing key regulatory roles, and with international cooperation being only partially developed, has important implications for critical infrastructure protection. It suggests that enterprises and public utilities responsible for managing critical infrastructure will have to look to themselves and their movements in the first instance for ensuring the integrity of their systems. System managers should consider what their international information requirements might be in the case of an attack and how these could best be obtained. In some cases, informal agreements might be adequate for gaining access to needed information across borders; in others, formal, inter-governmental agreements may be required. System managers should recognize that these formal information sharing agreements are not well-developed at the present time.

That fact, in turn, argues for security managers and executives who are well-equipped to follow the myriad regulatory developments now ongoing, and who are active--to the extent consistent with their other responsibilities--in the informal regulatory network that is so important not only

to technical standards, but to other issues as well. The IETF, for example, has played an active role with respect to the debate over encryption policy. Managers should be encouraged to be active participants in the relevant internet organizations, and in the associated policy debates.

REGULATING THE INTERNET

1. Introduction: National Security and the Global Economy

The global economy has always posed challenges to national security planners. Traditionally, national security concerns arose over dependence on foreign countries for natural resources and agricultural products--the raw materials needed for fighting a war. Policies for remedying that dependence included building stockpiles and diversifying among sources and suppliers. Later, governments began to fear that reliance on foreign countries and enterprises for high technology products would undermine their economic and military competitiveness. In this case, states provided financial support to domestic firms and universities for research and development, and in some cases they adopted protectionist policies in an effort to grow or at least maintain the domestic industrial base. Now, as we approach the 21st century, the global economy is posing a new set of challenges, which strike at the very heart of state sovereignty. Increasingly, policy analysts--and public officials themselves--have raised questions about the capacity of governments to manage their domestic and international relations in the face of an overwhelming increase--a virtual tidal wave--in global transactions and communications. Once again, governments seem to be losing control over their destinies, and their response has been to seek national and international regulations in an effort to ensure that globalization proceeds in a manner consistent with their vital national interests.

As these comments suggest, tensions between the global economy and the nation-state are hardly unique to our era. Writing on the eve of World War II, Professor Eugene Staley asserted that “fundamental technological changes are pushing mankind in the direction of world-wide economic integration and interdependence, but...political tendencies have strongly resisted that trend.”¹ Those political tendencies, of course, would soon explode into a war that placed nation-states very much at the center of international affairs.

A quarter-century later, in the midst of the “long peace” that followed the end of World War II, economist Richard Cooper renewed interest in the conflicts between nation-states and the international economy with his classic work, *The Economics of Interdependence*.² Cooper argued that countries were finding it difficult to strike a balance between their legitimate national objectives on the one hand and the exigencies of the global economy on the other. He concluded that the only way for movements to achieve their goals was through greater international policy coordination. The emerging European Community, of course, seemed to offer one potential model of how distinct nation-states might create new forms of governance in order to promote greater interdependence in a manner consistent with their military security concerns.

Since the end of the Cold War, and with the millennium in view, these tensions between the nation-state and the international economy have again come into sharp relief, this time most pointedly in discussions of the ever-expanding global information infrastructure (GII). In no sector of the economy do the seemingly anational and autonomous forces of “technology” and “the market” seem so strong, and the capacity of territorially-bound movements to harness these

forces seem so weak. But today there is a distinct difference, and that is the absence of any overwhelming military threat, at least to the member-states of the European Union (EU) and Organization for Economic Cooperation and Development (OECD). With national security concerns largely eroding in the “industrial” democracies, citizens are asking about the very purposes of the state and are debating its appropriate functions and spheres of activity. Indeed, governments cannot “play” the national security “card” as often as they once did, since today there are any number of societal actors who are now holding the even stronger hand of economic competitiveness and potential job creation. Because of the relatively benign threat environment, the state has lost some of its capacity for action.

Further, with advances in technology and our understanding of how markets function, it appears that non-governmental actors can satisfactorily provide a wide range of services which governments once monopolized. In one sector after another, long-held state and private sector monopolies are being dismantled, and new regulatory regimes are being constructed--some by the state, others by private agents. The telecommunications sector--which not so long-ago was government owned and managed in most industrial countries--of course represents a paradigmatic case of this development.

The global information infrastructure--and particularly the internet--provides a major arena for observing these changes in state-societal relations. On the domestic front, the net regularly pits advocates of civil liberties against those who would permit or even encourage the state to regulate and eavesdrop on private communications. In the international realm, the internet’s potential as a

vehicle for electronic commerce on the one hand, and criminal and terrorist activities of various kinds on the other, again pits free marketeers against those who would claim that governments have a justifiable role in regulating how the system is used, and by whom.

This report examines recent efforts by the U.S. government to promote international governance of the internet. Specifically, it focuses on international negotiations over encryption policy. The encryption debate brings together most of the salient regulatory issues facing the President's Commission on Critical Infrastructure Protection, and it demonstrates how the U.S. government is struggling to define an appropriate regulatory role in light of foreign governments and powerful domestic groups that have a wide array of conflicting preferences. Once an issue that was clearly defined in terms of national security interests, encryption today is more widely seen as the "golden key" to electronic commerce, which could open the door to a multi-billion dollar business; accordingly, few officials want to stand in its way. At the same time, the use of encryption technology by those who would seek to damage America's critical information infrastructure for economic, ideological, political, or criminal reasons means that some methods of access and control are needed which permit police and intelligence services to respond in a timely and forceful manner to any attacks. It is in this cauldron that encryption policy must be shaped.

The report proceeds as follows. In the following section, the differing models of regulation are analyzed. Section 3 provides a brief introduction to the GII, while in Section 4 two models of

internet regulation are described--private regulation of technical standards, and attempted public regulation of encryption. The final section provides conclusions and policy recommendations.

2. Models of Regulation

Since the mid-19th century, the role of government in most industrial societies has been characterized by explosive growth. Governments have been asked by their societies to take on a series of new tasks, driven by the demands of warfare on the one hand and social welfare on the other. In general, the rationale and locus for this governmental activity was clear: it involved the provision of so-called “public goods” to citizens living within the territorial boundaries established by the nation-state.

These regulatory functions and expenditures on public goods differed somewhat from country to country, but over time they more or less converged. Thus, countries regulated their money supplies, trade routes, domestic commerce, property rights, and monopoly suppliers like public utilities. They provided infrastructure and education. By the early 20th century, most of the industrial countries were also regulating social life in a variety of ways, as well as providing such welfare services as health care, unemployment insurance, and pensions. Later, governments established national parks and provided for environmental protection, notably clean air and water. Again, the objects of these public goods were the citizens of the country in question.

By some accounts, economic globalization is posing a challenge to this nationally-based, top-down governmental approach to regulation. According to British political scientist Philip Cerny,

“In a globalizing world, national states have difficulty supplying. . .(the) public good. Regulatory public goods are an obvious case. In a world of relatively open trade...property rights are more difficult for the state to establish and maintain. . .Currency exchange rates and interest rates are increasingly set in globalizing marketplaces. . .Legal rules are increasingly easy to evade...Finally, the ability of firms, market actors, and competing parts of the national state apparatus itself to defend and expand their economic and political turf through activities such as transnational policy networking and regulatory arbitrage. . .has both undermined the control span of the state from without and fragmented it from within.”³

This world-view naturally takes a grim view of the nation-state’s future. It sees governments as losing any real capacity to shape events within their borders--much less their international relations--, with power shifting to multinational corporations, non-governmental organizations of various kinds, or to even more decentralized, “virtual” networks, like the internet. It is perhaps not surprising that this image is particularly compelling in Europe, where the felt loss of sovereignty is especially acute with the evolution of the European Union, as it moves towards a single currency and perhaps soon to a single army as well. Yet this framework extends well beyond Europe; after all, no country has produced more globalization literature than the United States, a country that, presumably, should be more confident about its ability to manage its affairs than any other, given its relative economic insularity and its overwhelming military power.

In the event, this image of eroding state capacity has not gone unchallenged by other analysts. For example, taking the “hard case” of international finance--a sector that, like telecommunications, is

also known for its global, allegedly “anational,” and apparently uncontrollable operations--I argued in an earlier study that states have effectively responded to globalization through the development of *international cooperation based on home country control*.⁴ International cooperation refers to the myriad formal and informal agreements that states have reached with one another in an effort to supervise the marketplace; home country control refers to the responsibility that states have taken for defining their national enterprises and for regulating them. In banking, this means that every financial institution has one national regulator with primary responsibility for its supervision.

In its essence, regulation is always a matter of one agent seeking protection in some form against the actions of another. In most cases it exists to protect consumers from producers, but it also protects producers from potential competitors. In many cases the state itself has promoted regulation to protect its own interests against those of societal actors and the exigencies of the international system. When viewed in this light, we see that regulation is inevitably a contested terrain.

Regulation always requires three key ingredients: first, the formation of a “winning coalition” that authoritatively defines the nature of the problem at hand (e.g. monopoly pricing by a public utility); second, consensus about the appropriate solution (e.g. regulation of the utility’s pricing policy); and finally, an adequate provider of the solution (e.g. an independent public utility commission). The need for a new regulatory body or set of laws need not be universally agreed upon by everyone in society; in fact, it is inevitable that some individuals and groups will

question whether the alleged problem even exists, much less the necessity for any solution. Similarly, in the absence of any consensus among those seeking regulation about an appropriate solution and who should provide the regulatory service, it is unlikely that the regulatory movement can succeed. In short, those seeking regulation must be able to define problems and offer appropriate and proportionate solutions.

The case of global warming offers a useful example of both the promise and difficulties associated with attempted regulation. While a diverse group of scientists and activists has been fairly successful in defining the problem that exists (e.g. the greenhouse effect) and a solution (e.g. reduced “greenhouse gas” emissions), it has proved difficult to put any teeth into international agreements that would monitor and enforce national progress in reducing the emission of greenhouse gasses. Indeed, even the U.S. government, which has played the leading role in international environmental policy and the signing of the multilateral “Rio Treaty” on global warming, has stepped back from the earlier aggressive commitments to emission reductions that it had made. The problem for those who would seek to regulate greenhouse gasses is that there is simply no credible provider of this service other than the national governments themselves, and they tend to balance environmental concerns against other economic interests.

There is, of course, no a priori reason why governments must take the lead in regulatory matters. In fact, regulation may be provided by either the private sector or the government, and it can be either domestic, international or supranational in its purview. The matrix below, which takes several examples from the global information infrastructure, suggests the several possibilities:

A REGULATORY MATRIX

	Domestic	International	Supranational
Public	Encryption Policy	ITU/Intelsat	European Union Directives
Private	Domain Names Registry	Domain Names Allocation IANA*	Internet technical stds. IETF**/IAB***

*Internet Assigned Numbers Authority

**Internet Engineering Task Force

*** Internet Architecture Board

As we can see, both public sector and private sector regulatory arrangements exist with respect to telecommunications in general, and the internet in particular. What explains the difference between public and private sector regulation? Why can't all regulation be provided by the marketplace? In some cases, the answer is simply a matter of historical accident. In others, it is a matter of how close the issue is to traditional national security concerns; this would be the case of encryption policy. But from a more theoretical perspective, the answer would focus on problems of collective action. What this means is that those who seek a regulation may not be able to organize themselves in an effective manner. Take the case of public utilities regulation. An electric power plant or local telephone monopoly, for example, may serve many thousands of people, each of whom shares an interest in maintaining prices below monopoly levels. Let us imagine that I want to organize these consumers in such a way as to combat the utility's monopoly pricing practices. The costs of organizing such a large, diffuse group would be

prohibitive for me acting on my own, but at the same time only a very few consumers would likely have an interest in taking the time to work for my crusade against monopoly pricing, since the benefits of my victory would be shared among all consumers, no matter if they helped me or stayed at home. In such cases, the state may act on the behalf of all consumers, coercing their tacit participation in any regulatory scheme through taxation; private groups, of course, have greater difficulty in coercing participation from large numbers of individuals.

Related to the problem of collective action is the provision of public goods. States exist in large measure to provide public goods, like national security, which society demands but which the private sector will never produce, since it cannot capture all of the profits or benefits associated with such provision. Thus, some regulations, like environmental standards, take the form of public goods which benefit all citizens. The private sector would have little motivation to provide clean air acting on its own, since the costs of pollution control are concentrated while the benefits are diffuse.

In the private sector cases, in contrast, the benefits of regulation may be concentrated along with the costs. The setting of professional licensing standards by groups like the American Bar or American Medical Associations creates a monopoly practice which, while allegedly established in the broad public interest, increases the incomes of doctors and lawyers by restricting entry. Similarly, members of groups like the Internet Engineering Task Force may reap benefits (which could be non-monetary--for example, prestige) from setting technical standards which motivates them to provide this service.

The setting of domain names presents an interesting case in which domestic monopolies have been established in various countries (domain name registries), by an unofficial organization, the Internet Assigned Numbers Authority (IANA is not really an international organization, but it provides the international service of assigning national registry functions to particular domestic agents). In this case, the private monopoly clearly reaps benefits from its ability to assign domain names and charge for the service. Further, each of these national monopolies operates under different national rules--the setting of which also varies, some being more influenced by governments than others--since there is no international agreement on domain name access or pricing. Not surprisingly, this system has been deemed fragile by many observers, who expect that governments may ultimately play a more authoritative role in domain name regulation, including the setting of international standards. Indeed, the Organization for Economic Cooperation and Development (OECD) has already been closely following developments in this issue-area.

What determines whether these regulations are national, international, or supranational in scope?

The geography of regulation may be a function of technical issues (indeed, this approach is called functionalism), or it may be a reflection of underlying competitive and political conditions. Thus, public utility regulation would generally be a domestic matter, since most utilities face little if any international competition (this situation is of course changing as new technologies are introduced, with telecommunications again providing the paradigmatic case). In an area like banking, in contrast, financial companies face intense international competition, and in turn they have demanded of their national regulators a "level playing field" to the extent possible, in order to

ensure that national regulatory differences do not determine competitiveness; this demand, in turn, has fused with governmental concerns over the safety and soundness of the financial system to produce such international regulations as the Basle bank capital standards.

Internet standards, in contrast, are more of a technical nature; that is, the need for standards across borders stems from the need of different systems to talk with one another. The IETF and IAB determine standards across borders, and they do not represent particular national regulators with particular national interests. This method of standard-setting has evolved over time, growing with the internet. As MIT's Michael Dertouzos comments, "This approach (to the setting of technical standards) marked a major break in the way standards were formed. Instead of the top down process that took years to gel, the new groups operated in an informal manner, seeking advice, trying a quick idea here, giving out some code there, to seek if it 'took' and until it 'felt right.' This seemingly anarchic process moved the networking effort steadily forward."⁵

In contrast, the European Union is an example where supranational regulations originally came into being for political purposes, specifically the mutual desire of France and Germany to avoid fighting another world war. That narrow historic purpose has of course evolved substantially since 1957, when the European Community was created, but the politics remain firmly in place. Unlike the nets technical standards, the EU's supranational directives represent a long and difficult process of decision-making.

This framework provides a starting point for drawing some hypotheses about the likely evolution of internet regulation. These hypotheses are tested in the remainder of the study:

REGULATORY HYPOTHESES

H1: The more sensitive the issue is to national security, the more likely it is that the government will play the leading regulatory role.

H2: The more technical the issue, the more likely it is that the private sector will play the leading regulatory role.

H3: The more the issue involves income redistribution, the more likely it is that the government will play the leading regulatory role.

H4: The more the issue is characterized by international spill-over effects, the more likely it is that actors will pursue international regulatory agreements. If these issues involve questions of security or redistribution, the government will take the lead in international regulation. If the issues involve technical standards, the more important will be the private sector's role.

H5: The less agreement about the nature of the problem and solutions at hand, the less likely that any regulation will be produced by either the public or private sectors.

3. The Global Information Infrastructure

One of the major current objects of regulatory attention in every country and international organization around the world is the evolving global information infrastructure (GII). The GII,

while still lacking any precise definition, “incorporates several large communications and information components. First are the national telecommunications infrastructures. . .Next are the international cable facilities. . .Then comes the international satellite consortia. . .The GII also includes computer equipment, software and services, as well as the network standards, protocols and interfaces necessary to interconnect them...Summing up these components...revenues of the global information infrastructure totaled \$1 .35 trillion in 1993, or 5.6 percent of gross domestic product (GDP).”⁶ A report to President Clinton on the GII goes even further. It states that “the GII extends beyond hardware and software; it is also a system of applications, activities and relationships.”⁷

As the above dollar figure reveals, the impact of the GII on commerce, information gathering, and communications has already been substantial. But observers agree that its potential revenues are a significant multiple of that number. Electronic commerce is still in its infancy, while new methods of information gathering and retrieval are being developed almost daily. The efficiencies that the GII could eventually introduce in international business, science and technology, and even diplomatic relations might someday release billions of dollars for more profitable investments. Further, an increasing number of on-line services are switching from free to paid subscriptions. These potential developments suggest that the GII will be one of the most exciting sectors of economic activity for decades to come.

But the GII also poses a series of challenges to individuals, enterprises, and governments. Just as the technology is a force for free markets (and, by some lights, political democratization), it can also be used by criminal and terrorist elements to disrupt communications and transactions, or to

carry out illegal activities. Already the GII is used (how widely remains in dispute) by drug cartels, terrorist groups, and criminals of various stripes for such purposes as information transmittal, money laundering, pornography, and the spread of disinformation. Indeed, while most governments around the world have generally taken steps to liberalize the national information infrastructure and increase consumer access and use, control of these criminal information flows remains high on the policy-making agenda.

Despite these concerns, the U.S. government has actively and with rare exception (encryption technology being a partial case in point) advocated the spread of the GII. Indeed, the report to President Clinton on the GII suggested the following basic principles for guiding its future development:

- (1) Encourage Private Investment.
- (2) Promote Competition.
- (3) Provide Open Access.
- (4) Ensure Universal Service.
- (5) Create a Flexible Regulatory Environment.

The report made the following specific recommendations to governments with respect to GII regulation:

- a. Re-examine and adapt regulations and legislation to accommodate market and technological developments at national and global levels in support of the five GII principles;
- b. Create, through regulatory and/or legislative reform, a pro-competitive, technology-neutral

regulatory environment to maximize consumer choice, to provide fair access to networks, and to stimulate infrastructure development, the introduction of new services, and the wider dissemination of information;

- c. Exchange views and information on national regulatory and legislative initiatives and seek to identify common challenges and options for developing flexible and transparent regulations in support of the development of the GII;
- d. Work collectively in regional and international organizations to convene meetings devoted specifically to encouraging the adoption of regulatory policies that will promote the GII; and
- e. Encourage creation of independent national regulatory authorities for telecommunications separate from the operator that shall promote the interests of consumers and ensure effective and efficient competition.

The report also recognized that GII development must take into account privacy protection, security and reliability, and intellectual property protection. In each of these arenas, the need for international cooperation was acknowledged. In fact, efforts have already been ongoing in such organizations as the International Telecommunications Union (ITU), World Trade Organization (WTO), Organization for Economic Cooperation and Development (OECD), and World Intellectual Property Organization (WIPO) to hammer out international guidelines and agreements.

Even when we take these efforts into account, however, inter-governmental regulation of the GII, and specifically the internet, remains “underdeveloped.” That is, governments have had little success to date in reaching international agreements on such issues as content, domain name

registration, or encryption policy, where national differences prevail. Some observers believe that this failure to advance the process of international cooperation could eventually slow the GII's growth. According to MIT's Dertouzos, politicians must "ensure that agreements are struck across states and nations, because that is where the difficult battles will emerge and be fought. Following the models of international trade, telephony, and air transportation, all of which cross international boundaries, states and nations should now enter international agreements and adopt shared regulatory policies for handling trans-border information flows in the emerging global Information Marketplace. This will not be easy, but it must be done... Such agreements will help us maintain some order as we make the transition to the new world of information."⁸ In the following section, private sector and public sector regulatory approaches to the internet are compared and contrasted, in an effort to understand the problems and possibilities associated with international cooperation.

4. Regulating the Internet

As the comments provided above have already suggested, there are several broad approaches which could be adopted in theory to regulating the internet. First, nation-states could seek to provide the regulatory focus, amending existing laws and regulations and writing new ones as necessary. This model of "home country control" is widely used as the cornerstone of international regulation in many issue-areas, from finance to telecommunications. Indeed, in a global economy, it is tempting for authorities in country A to seek one regulator in country B who is responsible for supervising the overall activities of multinational firms.

Second. and complimentary with the first approach, countries could seek to develop international or multilateral agreements. Again, there are a wide variety of existing regulatory bodies that could presumably expand to incorporate internet regulations among their existing functions.

Third. countries could opt for the creation of a new international or even supranational organization which would establish new rules and operating procedures for the internet. In order to be effective, this body would also have to possess the authority to sanction parties that were not playing by the rules of the game.

Fourth, governments could do nothing, anticipating that internet rules would arise spontaneously (many of societies deepest regulatory structures, like marriage, apparently arose “spontaneously”) through the action of interested groups banding together to promulgate regulations that users view as being acceptable. Indeed, this process has largely been responsible for the evolution of technical standards on the internet.

The first three methods are ah familiar to public officials and some combination of them might seem at first glance to offer the best hope for solving the regulatory problems now arising on the net, including issues of content, domain name registration, and secure transactions (especially through encryption). But the latter, “anarchic” approach should not be dismissed out-of-hand, and merits some serious consideration. It may be that internet technology, which acts to decentralize information flows and decision-making processes in many important respects, also requires a decentralized regulatory apparatus. However, we would do well to recall the plea of Michael

Dertouzos, cited above, that governments act to regulate the net, in order to avoid “chaos.”

Indeed, the very question that the informal approach to regulation poses is whether anarchy” must inevitably lead to “chaos,” or whether it can bring about order spontaneously in the absence of a dominant and coercive agent.

The history of telecommunications regulation suggests the variety of approaches that have already been adopted for the GII’s precursors. When telegraphy first crossed borders, for example, “there were many technical incompatibilities and service coordination was necessary to effectuate cross-border communications.”⁹ Initially this took the form of bilateral agreements, and later regional arrangements, such as the Western European Telegraph Union, were formed. In 1865, however, Napoleon III convened a meeting in Paris which established the International Telegraph Union. This new organization had as its objectives system interoperability, along with methods for settling cross-border accounts. Eventually, the ITU became an arm of the United Nations.

Of interest, when telephones came into widespread use, the ITU took the decision not to regulate it initially, “for fear of stifling the technology.”¹⁰ Only in 1925 did the ITU form separate committees to study telephone technology and tariff issues. The model eventually adopted for telephone regulation--”home country control”--persists today, despite the globalization of telecommunications. That is, home countries have ultimate supervisory responsibility for their telephone systems, although a number of international agreements now exist to facilitate cross-border communications.

The manner in which the internet will ultimately be governed still remains an open question. Most likely, there will be no single national or international regulator for the infrastructure as a whole. Instead, it will be regulated in different ways by different actors in different venues, according to the issue at stake. That mixed approach is already evident. Technical standards for the net, for example, are governed by an informal body, the Internet Engineering Task Force (IETF), which acts de facto as a supranational body. Encryption policy, in contrast, has been the domain of nation-states, and international agreements are proving elusive. There is no a priori reason why the internet cannot continue to be regulated in this diverse fashion, at least for the foreseeable future, with the regulatory response depending upon the “issue-area.” To be sure, it is not a very neat solution, and will likely mean a great deal of overlap among “regulators” in the public and private sectors with respect to the borders of their responsibilities. Conflict among these regulators and the interest groups behind them is inevitable. But given the technology and its diverse uses, and the differences in national preferences with respect to such issues as acceptable internet content, this may be the only approach that works. It is critical to recall that regulatory policy will only be effective when the issue at stake is “ripe” for a regulatory solution, again meaning that an authoritative definition of the problem exists, along with an appropriate, proportionate solution and an actor capable of enforcing that solution. In the absence of this setting, regulations will either be debated but not established, or established but remain ineffective.

a. Non-governmental Regulation

In many ways, the internet can be conceptualized as a solution to the problem of “how to get large numbers of individual computer networks, running diverse operating systems, to communicate with one another...”¹¹ While initially developed by the U.S. government as a method for solving communication problems during nuclear attacks (ARPANET), it soon evolved into a number of competing systems. Potentially, these systems might not have been interoperable, but through the establishment of voluntary agreements reached in informal settings, as provided by the Internet Engineering Task Force (IETF) for example, “destructive” competition has been avoided.

This point deserves emphasis. The internet has developed in order to permit different system providers to interact with one another. This networking process demanded that difficult technical decisions be taken that each party viewed as being in its interest. These decision-making procedures were first established by the U.S. government, but have since devolved to an informal, non-governmental body, the IETF, and its sister organizations.

Governance of technical standards is the provenance of four bodies: the Internet Society (ISOC), the Internet Architecture Board (IAB), the Internet Engineering Steering Group (IESG) and the IETF. According to a brief history of governance issues prepared by IETF, the organizations divide responsibilities as follows:¹²

The Internet Society is a professional society that is concerned with the growth and evolution of the worldwide Internet, with the way in which the Internet is and can be used, and with the social, political, and technical issues which arise as a result. The ISOC Trustees are responsible for approving appointments to the IAB from among the nominees submitted by the IETF nominating committee.

The IAB is a technical advisory group of the ISOC. It is chartered to provide oversight of the architecture of the Internet and its protocols, and to serve, in the context of the Internet standards process, as a body to which the decisions of the IESG may be appealed. The IAB is responsible for approving appointments to the IESG from among the nominees submitted by the IETF nominations committee.

The IESG is responsible for technical management of IETF activities and the Internet standards process. . . The IESG is directly responsible for the actions associated with entry into and movement along the Internet “standards track,” including final approval of specifications as Internet Standards.

The IETF is divided into eight functional areas. . . The area directors, along with the IETF/IESG Chair, form the IESG.

As this suggests, a complex but authoritative regime for technical standards has guided Internet development.

Still, the boundaries among the organizations are by no means clear-cut, and it is possible that the existing structure will be overwhelmed by the demands placed upon it. As the IAB has recently reported, “the boundaries of the proper role for the IETF, the IESG and the IAB are somewhat

fuzzy.” Further, the IAB has found itself getting involved in other issues, like domain name registration, which are also being handled by other groups (for example JANA and the various domestic domain name registries). Beyond this, the internet of course interacts increasingly with other technologies that are part of the “information infrastructure.” This raises the question for IAB of “how far up or down do we go?” Clearly, “the boundary between IETF standardization” and other technical specifications “can never be rigid.”³

The evolution of regulation of technical standards provides a strong case study of “spontaneous” regime creation. Rather than create a government-led and directed response to the problems posed by interconnectivity, the system has developed a “decentralized” form of collective action which “involves voluntary acceptance of standards. Despite the fear of those who cannot conceive of order as arising from anything other than top down, hierarchical control, this is not a process that necessarily leads to chaos and anarchy. . . decentralized action may well be capable of generating responsible self-regulation of the net...”⁴

One question that the apparently successful case of informal, technical standards setting raises is its applicability to other net-wide issues, such as content regulation, domain name registration, or encryption. In other words, could net-wide governance be left to the private sector in the hope that structures like the ISOC/IAB/IETF/IESG quartet emerge to solve collective action problems? There are several reasons why we should not be optimistic about the possibilities of transferring this model.

First, it should be recalled that the IETF was originally created and funded by the U.S. government. Theorists of international regulation have pointed out the important distinction between “regime creation” and “regime maintenance.”⁵ Movements are often necessary in order to launch regulatory regimes, because only they can overcome collective action problems in part because of their ability to coerce cooperation. Once these regulatory regimes are established, however, they can be maintained by marketplace actors, who views them as being in their interest.

Again, the case of capital adequacy standards for banks provides a good example of this distinction. Initially, a set of capital adequacy standards were developed and enunciated by bank regulators from the Group of Ten countries as a way of increasing the safety and soundness of the international financial system. While each national regulator had previously taken a unique approach to bank capital adequacy, given the particular banking structure in that country, they recognized that capital standards should not be the basis upon which banks (or countries) competed for financial business, since this could only lead to a downward spiral that would threaten the system’s viability. Accordingly, these regulators established specific standards that all international banks would be expected to meet. Once these standards were established, however, the marketplace largely took over in ensuring that they were being adopted. Credit rating agencies and investment banks published reports telling how well the banks were doing, and they priced their debt and equity offerings for the banks partly as a function of how close the banks were to the “Basle” standards. Conversely, banks that did not meet these capital adequacy standards were punished in the marketplace by falling stock prices or less business.¹⁶

The lessons of the “Basle agreement” on bank capital should not be lost on those who imagine that the internet will solve all its regulatory problems on its own. In many cases, official, governmental action is needed to create a regulatory framework. Certainly, banks acting out of their own self-interest could not have been expected to craft a collective agreement on capital adequacy. At the same time, government officials should recognize that in many regulatory cases their most important function may be a catalytic one, and that new bureaucracies and complex laws are not always needed to meet the objectives they seek.

b. Attempted International Cooperation: Encryption Policy

A very different approach to internet regulation has been taken in the case of encryption policy. In this issue-area, which sits very close to governmental concerns over national security, states have traditionally played a leading role in seeking to control the diffusion and use of this particular technology. As encryption becomes more widely used as a tool of electronic commerce, however, and as it becomes less expensive (even free!) and more accessible through the internet and other sources, a new set of pressures is acting upon regulators. The debate over encryption policy comes down to this: can national security, privacy, and free market concerns be reconciled in a way that meets everyone’s interests?

The emergence of encryption as one of the most critical and contested regulatory issues facing the internet points to its unique role in the information age. As a recent expert report puts it, “Encryption is an essential tool in providing security. .Properly implemented encryption allows sensitive information to be stored on insecure computers or transmitted across insecure

networks.” Beyond the transmission of sensitive information, cryptographic techniques “can be used to guarantee that the contents of a file or message have not been altered (integrity), to establish the identity of a party (authentication), or to make legal commitments (digital signatures).” The secure use of encryption is thus absolutely vital to the expansion of electronic commerce. At the same time, advanced cryptography makes it “more difficult for law enforcement to conduct certain kinds of surreptitious electronic surveillance. . .This difficulty is at the core of the debate” over encryption policy.¹⁷

For most of its history, cryptography has been the province of the nation-state. Advances in cryptography were driven by the national interest in achieving secure military and diplomatic communications (one of its great inventors was Leonardo Da Vinci, who crafted cryptographic techniques for his royal masters). As the private sector began to develop encryption techniques for its own uses, the US government sought to develop a new approach—escrowed encryption—“that would provide strong protection for legitimate uses but would permit access by law enforcement officials when authorized. . .Today, these and other dimensions of current national cryptography policy generate considerable controversy.”¹⁸. Indeed, cryptography provides a fascinating case study of a highly technical issue-area which has become a battle-ground for a wide array of competing interests; as a result, it has now also become an issue of substantial legislative concern, as Congress tries to develop laws that reconcile these groups. Further, it has now entered the international agenda, since differing national laws on encryption have both competitive and national security effects.

Encryption is sometimes described as the golden key that will enable electronic commerce to flourish, through its ability to protect consumer transactions. At the same time, it is described as the ultimate lock on the door, protecting critical information against attempted break-ins. While encryption's benefits for information security are obvious, the technology also risks being oversold as a panacea for solving the internet's security problems. In most of the cases reported to date, stronger encryption technology would not have prevented consumers or firms from being ripped off, or critical infrastructure from being violated by hackers or criminals.

This point may be emphasized by taking one of the most famous cases of a "break-in" of an encrypted system. In 1994, Citicorp discovered that a criminal gang with strong roots in Russia had entered its electronic money transfer system, withdrawing \$400,000 before being caught. The gang did not enter the system through its superior ability to break the Citicorp code. Instead, it "allegedly penetrated Citicorp computers using customers' user identifications and passwords." A gang member, Vladimir Levin, "electronically impersonated a legitimate customer..." Further, "some investigators suspect that an accomplice inside Citicorp provided. . . necessary information; otherwise it is unclear how he (Levin) could have succeeded in accessing customer accounts."¹⁹

This case study illustrates that good old-fashioned fraud, blackmail, and greed will continue to play major roles in disrupting even the most secure systems.

Indeed, the real danger might be that encryption could provide some users with a false sense of security. Given the difficulties of breaking strong encryption, it is easy to imagine that some administrators will be lulled into thinking that their systems cannot be breached. As a result, it may take longer to detect any malfeasance. By that time, substantial damage could already have

been done. In the words of security expert Peter Neumann, “We’re just waiting for the massive fraud that takes down a brokerage house or Internet company.”²⁰

Governments have sought to limit access to encryption through import controls, export controls, and use controls.²¹ In the United States, the most important category concerns export controls; in practice, import controls have not been widely used, and “like most western countries, the United States does not control domestic use of strong encryption.”²² It should be noted, however, that export control restrictions can effectively limit domestic use of a technology as well, since a software company (eg Microsoft) may not wish to produce different software packages for its domestic and foreign customers, much less have to worry about foreign customers buying their software packages in the United States and then bringing them home without the appropriate export license.

Until recently, encryption technology was included on the munitions list of the State Department, but the Clinton Administration has shifted export control responsibility to the Department of Commerce in an effort to signal its market-friendly intentions. Still, the administration has been unable to strike a balance between market and national security interests pleasing to all sides. A recent trip to Capitol Hill by Bill Gates and other leading high-tech executives represented a major effort to loosen existing restrictions on the export of encryption technology, and several congressmen are now expressing open support for their perspective.²³

To the government, the use of strong encryption products poses a potential threat to national security. As President Clinton said in his official statement on encryption policy, “encryption

products, when used outside the United States, can jeopardize our foreign policy and national security interests...The exportation of encryption products accordingly must be controlled to further US foreign policy objectives. and promote our national security, including the protection of the safety of US citizens abroad.”²⁴

In recognizing the economic interests of American companies in exporting encryption technology, while at the same time respecting national security and police requirements, the administration has attempted a two-pronged approach. On the one hand, it has coupled the loosening of export controls to the establishment of “key recovery” systems which would give the government access to cryptographic keys; there has been considerable policy movement in recent years over what this key recovery system would actually entail, as discussed in more detail below. On the other, it has launched an effort to promote international cooperation on encryption policy in order to make the world safe for the inevitable increase in encrypted communications that will come with the expansion of electronic commerce. Specifically, it has sought to establish international guidelines which could ultimately result in the creation of a global key management infrastructure. but which in the meantime has the more modest objective of pressuring movements to ensure that the net is not being used for criminal purposes within their own territorial boundaries.

The Clinton administration’s devotion to a key management approach is of long-standing. Originally, it took the form of offering firms and individuals access to strong encryption through a “clipper chip,” for which the government would hold a master key that could decrypt coded messages. This proposal soon fell by the wayside in the face of public opposition. Subsequent

versions, though, took the more sophisticated form of “key recovery/key management” systems, in which encryption keys would be entrusted to “certified” third parties within or outside a particular firm or government agency. According to one governmental draft paper, “public key cryptography must be based on a key management infrastructure and attendant products that tie individual and corporate identities to their public key through a series of Certificate Authorities (CA). The key management infrastructure to do this on a global scale will be very large and complex, *but it is an essential foundation* (emphasis added).”²⁵ This key management approach remains at the core of the Clinton Administration’s effort to reconcile commercial and national security concerns.

Despite the administration’s effort to loosen export controls in the context of a key recovery plan, market actors have responded negatively to this government initiative. The market’s perspective is that strong encryption technology--much of it without key recovery plans is already widespread, and that “export controls place companies in that country at a competitive disadvantage.”²⁶ According to a joint-statement by the IAB and IESG, a key recovery infrastructure--as proposed by the Clinton Administration--“inevitably weaken the security of the overall cryptographic system, by creating new points of vulnerability that can and will be attacked.”²⁷ Further, experts argue that governments and firms have very different needs when it comes to key recovery. Governments, they argue, seek the following:

- (1) “Third party/government access without notice to or consent of the user.”
- (2) “Ubiquitous international adoption of key recovery.”
- (3) “High-availability, around the clock access to plain text...”
- (4) “Access to encrypted communications traffic as well as to encrypted stored data.” Firms,

they say, do not share these same objectives, and would put into place very different security systems than those proposed by the government in order to meet their specific requirements.²⁸

The Administration's devotion to the key recovery approach, however, was seemingly highlighted once again in its recent decision to approve "the export of the strongest available data encryption products to support electronic commerce around the world.. .New regulations will be published to allow the export of products specifically designed to support financial transactions. These include direct home banking software of any key length, offered by banks to their customers worldwide. The regulations will also allow exports, for two years, of powerful, non-recoverable, commercially available data encryption products when used for inter-bank and similar financial transactions, once the manufacturers of commercial products file a commitment to develop recoverable products. "29

In granting this approval, the administration emphasized that it means to establish "a robust security infrastructure that will permit users from homes and businesses to perform all types of commercial data transactions. . .That infrastructure will manage encryption and digital signature keys to provide privacy, message integrity, user authentication, and recovery services. The Administration remains committed to key recovery, a market-drive approach which balances the need for strong security for electronic information with the need to preserve the ability of law enforcement agencies to investigate and prosecute serious crimes."³⁰ Curiously, however, key recovery was *not required* for financial specific products, since existing laws already guarantee

law enforcement officials access to financial transaction information when authorized. Some observers have wondered whether this represents a back-pedaling of the administration's position with respect to key recovery.

As has happened in other regulatory cases (e.g. regulation of bank capital), the administration has also tried to win support for its key recovery approach to cryptography by seeking an international consensus around this security architecture. In that way, a "level playing field" is established for cryptography producers and users. If complaints were earlier lodged that export controls place certain firms at a competitive disadvantage, then these should be silenced by an international agreement. At the same time, it is believed that an international agreement could facilitate the spread of global electronic commerce.

The administration's international effort had its "official" kick-off in November 1996, when Vice President Al Gore announced the appointment of David Aaron, U.S. Ambassador to the Organization for Economic Cooperation and Development, as Special Envoy for Cryptography. Indeed, that same day, Gore announced that jurisdiction for export controls on encryption products was being moved from the State Department (and its munitions list) to Commerce, and of course these events were intimately related. As Gore said at the announcement, "These two actions will help to promote the growth of international electronic commerce and robust secure global communications in a manner that protects the public safety and our national security."³¹ In fact, underpinning these two actions was key recovery; since it was that technology which allowed the administration to believe that it could solve its national security and electronic commerce concerns with a single initiative.

Since his appointment, Ambassador Aaron has been traveling to various capitals trying to secure some guidelines--and ultimately an OECD agreement--with respect to encryption technology. Naturally, these guidelines would preferably take the form already outlined by the US government, meaning that relaxation of export controls would be coupled to the development of a key recovery and key management infrastructure. While he has made some progress in that direction, serious technical questions have lately come to the fore which question the feasibility of this general approach, and indeed the ultimate OECD document would considerably water-down the key management concept.

In fairness to the U.S. approach, some cryptography specialists had earlier touted the potential value of key management schemes. For example, in one widely cited paper, scholars from the University of London's Information Security Group proposed a "novel mechanism that will enable TTPs (trusted third parties) to perform the dual role of providing users with key management systems and providing law enforcement agencies with warranted access to a particular user's communications." It was admitted, however, that the proposed approach would not work for "integrity, origin authentication or non-repudiation services."³² In other words, its overall value was limited. Still, government officials who launched the export control/international coordination initiative undoubtedly believed that reasonable technical solutions to key management issues were close at hand, if not already available.

More recently, however, specialists have expressed their doubts about the feasibility of a global key recovery system. According to a recent report by a group of leading experts in the field of encryption, "Building the secure infrastructure of the breathtaking scale and complexity

demanded by these requirements is far beyond the experience and current competency of the field. Even if such an infrastructure could be built, the risks and costs of such a system may ultimately prove unacceptable.”³³ Indeed, they point out that there is no economic model yet developed which has estimated the costs of building a global key management infrastructure, or how the charges would be assigned to users.

In the face of these objections, and owing to the fact that most other OECD governments simply do not have well-developed cryptography policies at this time, the Aaron initiative has not yet resulted in any meaningful international regulations. Instead, it has resulted in a draft set of rather general OECD guidelines. The guidelines for cryptography policy are as follows:³⁴

- (1) Trust in Cryptographic Methods: “Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems.”
- (2) Choice of Cryptographic Methods: “Users should have a right to choose any cryptographic method, subject to applicable law.”
- (3) Market-Driven Development of Cryptographic Methods: “Cryptographic methods should be developed in response to the needs, demands, and responsibilities of individuals, businesses, and governments.”
- (4) Standards for Cryptographic Methods: “Technical standards, criteria, and protocols for cryptographic methods should be developed and promulgated at the national and international level.”
- (5) Protection of Privacy and Personal Data: “The fundamental rights of individuals to privacy. . . should be respected in national cryptography policies...”

- (6) Lawful Access: “National cryptography policies may allow lawful access to plain text. or cryptographic keys, of encrypted data...”
- (7) Liability: “...the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated...”
- (8) International Co-operation: “Governments should co-operate to co-ordinate cryptography policies. . .*If developed, national key management systems must, where appropriate, allow for international use of cryptography* (emphasis added).

As we can see, the guidelines do not offer any explicit support for the development of a global key management infrastructure.

Accordingly, the OECD document has been “widely seen as a defeat for the United States...” While other observers would not go this far, even a lawyer on the U.S. delegation admitted that the document did not offer “a clear statement one way or the other” with respect to key recovery. Still, all sides agree that the process initiated by Aaron has catalyzed international discussions on encryption policy, and this will likely make it easier for the FBI and other national police organizations to cooperate across borders with respect to encrypted communications.³⁵

The story of encryption policy points to one of the regulatory hypotheses pointed out in an earlier section of this report: that in the absence of substantial agreement about the nature of a given problem and the appropriate solution, it is unlikely that a regulatory response will be developed. Simply stated, encryption policy is not yet ripe for a neat international solution. The problem with the approach taken by the Clinton administration towards encryption policy was not its argument

that the widespread use of encryption posed important issues of national security--no sensible person would dispute that assertion--but rather its implicit suggestion that the problem facing the government was so grave that it warranted jeopardizing what many Americans consider to be their fundamental civil rights. Further, the solution that the government has offered to date--key recovery--has proved to be much more elusive than initially imagined. Today, many leading experts have expressed serious doubts about the feasibility of establishing a secure key recovery system on the domestic level, much less on the international one.

Still, electronic commerce will not fulfill its promise until a secure and private infrastructure is established. Further, encryption must be at the core of this effort. This suggests that a two-track approach may emerge in which multinational enterprises and others engaged in electronic commerce develop their own secure systems, while governments continue to rely on national technical means, informal agreements with enterprises, and other methods to eavesdrop and gather information on encrypted communications, including ad hoc international agreements to track criminals. Indeed, even MIT's Dertouzos, who is an advocate of international regulatory cooperation, writes with respect to electronic crime that "police and other authorities will need to adapt their techniques. . . . But the broad framework in which they perform these jobs can remain the same. "36 This may be an over-statement, but it does suggest that the current system is not without merit until a more elegant international solution emerges than those presently under discussion.

One potential problem with this two-track approach, incidentally, is that it would likely benefit "trademark" names in the world of electronic commerce, since consumers are likely to have more

confidence in the encrypted systems provided by “Fortune 500” type firms as opposed to those offered by small business. To the extent that governments will want to encourage small businesses to play a major role in the world of electronic commerce, they will wish to pay attention to this issue, as some have already done. For example, the development of “trusted third parties” for key escrow/key recovery, such as major banks, might provide a model for how small firms could “borrow” goodwill from larger companies when it comes to the security of encrypted systems.

To the extent that international cooperation develops in the area of encryption policy, it will be largely a reactive and incremental process: a response to developments—and problems—actually occurring on the net. With respect to electronic commerce, countries will act to facilitate transactions that are in the interests of their international firms, and if this requires formal agreements, these will inevitably take shape over time. Observers may be surprised, however, by how much electronic commerce can develop given the present state of encryption technology and international understandings, both formal and informal. With respect to national security, ad hoc bilateral agreements will probably be the most prevalent means for information gathering across borders for the foreseeable future. In fact, since “the requirements of a government and the requirements of the commercial world.. .are very different” when it comes to encryption, this mix of official and informal regulatory approaches may be the most sensible one for all parties to the encryption debate to encourage at the present time.³⁷ Still, incremental efforts to develop international cooperation should continue, for eventually these may provide the seeds for more robust agreements. In short, efforts to advance international cooperation should not wait for the next crisis.

5. Conclusions and Policy Recommendations

The tremendous growth in global communications and transactions has led some observers to suggest that states are losing the capacity to manage their domestic much less international affairs. The spread of technology and information has seemingly created a borderless world in which governments are largely irrelevant. Further, the end of the Cold War and the erosion of the threat environment has placed the core function of the state--the provision of national security--into doubt. These background conditions would not appear to provide a very promising basis for the creation of an effective regulatory environment for the rapidly evolving internet.

But as this report has argued, the internet does not function in a borderless world without any rules. Instead, it is regulated by many different bodies at many different levels. On some levels, informal agreements struck by non-governmental organizations have proved extremely effective. On others, national authorities assume a variety of regulatory functions. These actors and the rules they have created have enabled the rapid and widespread growth of the internet. Without these agents and policies, the internet would have been stymied.

However, formal international bodies have seemingly had a more difficult time striking effective international agreements. That should be puzzling to GII observers (and participants), for if the internet is borderless, it would seem that international organizations would assume more importance than ever before in regulatory activities. Why hasn't this been the case?

This report would point to two major answers. First, many issues confronting the net are simply not “ripe” yet for international agreement. That is, international understanding of the problem, much less the solution, does not yet exist. This may be because use of the net is still in its infancy in many countries, or because different societies simply disagree about issues like content legislation. In such cases, national rules will continue to apply for the foreseeable future.

Second, in a globalizing world, states (paradoxically) become all the more central as the proper locus for regulatory activity. This is because states can only look to one another--and not yet to any supranational information body--to enforce existing rules of the GII and restrain criminal activity that would threaten its ability to function. This model of “international cooperation based on home country control” is pervasive in many issue-areas of the global economy, from oil tanker pollution to telecommunications policy to financial regulation. It appears to be the model that the internet is following as well.

That does not mean, of course, that states must play the lead role in providing regulatory services. As we have seen, a variety of non-governmental actors seem to be doing an adequate job at present of providing a wide variety of needed rules and operating procedures. Having created a set of property rights and a working judiciary, states may be able to withdraw from a wide-range of regulatory functions which they once monopolized. At the same time, we can expect that state services will still be required as electronic commerce and other activities evolve on the net, and that issues which today are non-governmental may, over time, be taken over by state authorities. In some cases, private sector actors may simply lack the capacity needed to continue providing regulatory services as the net grows, and they will seek to hand these responsibilities over to

governments, so long as the state retains its capacity to coerce participation in any regulatory schemes through its ability to tax its citizens.

These points suggest the need for a flexible policy stance on the part of government. This, in turn, means that the government must act to retain technical people who are capable of following the GII's development and who can participate in such informal regulatory structures as established by the IETF/IESG/IAB framework. It argues for the importance of education and training of government managers with responsibility for GII oversight and supervision. And it also points to the utility of the American system whereby professionals from university and enterprise settings enter government service for relatively brief periods of their careers.

With specific reference to the problem of critical infrastructure protection, this report has argued that those public utilities and private enterprises that operate such infrastructure should not be overly confident in the ability of encryption technology to meet their security needs. To be sure, strong encryption is a powerful tool which is a vital necessity for safeguarding secrets and preserving system integrity and user authentication. But many if not most cases of "break-ins" of critical infrastructure systems come down to old-fashioned fraud, blackmail, and lying done from the inside. While this points to the strength of these systems in terms of defense from outside attack, we still have a long way to go to develop methods--consistent with respect for privacy and civil liberties--that provide users with confidence that those employees who are responsible for maintaining critical infrastructure are absolutely trustworthy.

To be sure, in defending the world's critical infrastructure, international agreements of various kinds will someday prove necessary so that executives and officials can share information in a timely manner. Managers of critical infrastructure should thus think carefully about what their requirements and responsibilities in the international setting are likely to be. What information might they need to access overseas, and what information might they be called upon to provide? How can they verify the requests and the information that come their way? In the absence of formal international agreements, how can these requirements and responsibilities best be met? These are among the questions that have become common in the "virtual" world of the internet, but the answers are still being formed. In the meantime, we can only hope that incremental efforts to build international cooperation will be a continuing process, and not one that gathers force solely in response to the next major crisis.

NOTES

1. Staley, *World Economy in Transition* (New York: Council on Foreign Relations, 1939), p. vii.
2. New York: McGraw-Hill, 1968.
3. Philip Cerny, "Globalization and the Changing Logic of Collective Action," *International Organization* 49 (Autumn 1995): 595-625, at 609-610.
4. Ethan B. Kapstein, *Governing the Global Economy: International Finance and the State* (Cambridge, Ma.: Harvard University Press, 1994).
5. Michael Dertouzos, *What Will Be* (New York: HarperCollins, 1997), p. 40.
6. Walter Baer, "Will the Global Information Infrastructure Need Transnational (or any) Governance?," processed, nd.
7. National Academy of Sciences, "The Global Information Infrastructure," 29-30 March 1995.
8. Dertouzos, *What Will Be*, p. 292.
9. L. Raveendran, W. Hui, B. Greene, "The Three C's of Cyberspace: Competition, Collaboration, or International Cooperation," processed, nd.
10. Ibid.
11. David Johnson and David Post, "And How Shall the Net be Governed?" processed, 5 July 1996.
12. "The Tao of IETF," processed, nd.
13. Brian Carpenter, "What Does the IAB Do, Anyway," processed, nd.
14. Johnson and Post, "And How Shall the Net be Governed?"
15. Robert Keohane, *After Hegemony* (Princeton: Princeton University Press, 1984).
16. For the details, see Kapstein, *Governing the Global Economy*.
17. Hal Abelson, et.al., "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption," 21 May 1997.
18. National Research Council, *Cryptography's Role in Securing the Information Society* (Washington. DC: National Academy Press, 1996), p. 4.
19. Cited in NRC, *Cryptography's Role*, p. 23.
20. Cited in Jane Bryant Quinn, "Improving Security for Online Commerce," *Washington Post*, 27 October 1996.
21. Baker, "The International Market for Encryption," Presentation to the Symposium on Information, National Policies, and International Infrastructure, Kennedy School of Government, 30 January 1996.
22. Baker, "The International Market."

23. Elizabeth Corcoran, "Microsoft's Bill on Capitol Hill," *Washington Post*, 5 June 1997.
24. The White House, "Encryption Export Policy," 15 November 1996.
25. Bruce McConnell and Edward Appel, "Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure," 20 May 1996.
26. "IAB and IESG Statement on Cryptographic Technology and the Internet," 24 July 1996.
27. Ibid.
28. Abelson, "The Risks of Key Recovery."
29. Commerce News, "Encryption Exports Approved for Electronic Commerce," 8 May 1997.
30. Ibid.
31. The White House, "Vice President Announces Special Envoy for Cryptography," 15 November 1996.
32. Nigel Jeffries. Chris Mitchell, Michael Walker, "Combining TTP-based Key Management with Key Escrow," Information Security Group, University of London, 19 April 1996.
33. Hal Abelson, et.al., "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption," processed, 21 May 1997.
34. OECD, *Draft Recommendation of the Council Concerning Guidelines for Cryptography Policy*, 11 March 1997.
35. Joel Deane, "The Great Crypto Arm-Wrestle," 16 April 1997, www.thesite.com
36. Dertouzos, *What Will Be*, p. 289.
37. Abelson, et.al., "The Risks of Key Recovery."