



THE GLOBAL INFORMATION SOCIETY PROJECT

A RESEARCH COLLABORATION OF THE WORLD POLICY INSTITUTE AND THE
CENTER FOR ADVANCED STUDIES IN SCIENCE AND TECHNOLOGY POLICY
WWW.GLOBAL-INFO-SOCIETY.ORG

THE PROGRAM ON TELECOMMUNICATIONS AND CYBERSECURITY POLICY

Overview: Telecommunications is a vital component of our national infrastructure and plays an important role in national security. The telecommunications industry provides direct communications services to consumers, industry, and government, and these services and the underlying telecommunications infrastructure are significant factors in maintaining modern economic and social life. Indeed, many industries - for example, media and finance - would be impossible to maintain in their current form without modern telecommunications services. Others - for example, retail and manufacturing - could not function at the scale and with the efficiencies of current operations without these services. Government itself would be hard pressed to maintain routine public services or order without advanced telecommunications networks. And, robust telecommunication services are needed to manage national defense, disaster response, and other emergency services.

The Program on Telecommunications and Cybersecurity Policy is concerned with issues relating to (1) protecting and maintaining a resilient telecommunications industry and infrastructure, (2) protecting against or responding to cyber attacks on telecommunication, network, or computer infrastructure, and (3) regulatory policy relating to telecommunications infrastructure and spectrum management, ownership, and control.

Infrastructure Protection and Resilience:

Economic and national security require resilient communication networks - that is, networks that can withstand damage and continue to provide service in face of direct physical or cyber attack, natural disaster, or other disruptions. Network resilience requires strategies (1) to protect against or avoid failure; (2) to minimize, localize, or otherwise contain failures that do occur in order to avoid collateral or residual damage; and, (3) to repair, route around, or otherwise respond to failures in order to continue service. Achieving resilience requires investing in security, redundancy, and interoperability.

Since over 90% of telecommunication infrastructure is in private sector hands, government policy mechanisms are needed to influence private firm behavior in areas where market externalities inhibit sufficient investment in resilience or inter-firm cooperation, particularly where the consequence of failure has national effect. Available policy mechanisms include direct regulation, technical standards, insurance requirements, immunity and liability policy, tax incentives, market mechanisms, government as a lead user, and others.

Cybersecurity:

In addition to physical attack or natural disaster, the telecommunications networks and computer infrastructure required to support information-based economic and social life in modern economies is also subject to cyber-attack. Cyber-attacks can be malicious or accidental; can involve attacks by other nation states, organized groups, or individuals; and can be motivated by monetary gain, ill-will, or political interests. Cyber-attacks can be directed at governments, firms, or individuals. Cyber-attacks can involve the theft or destruction of information; the theft of services or financial assets; or the destruction of hardware or software infrastructure. Cyber-attacks can result in financial loss, business or service interruption, or infrastructure destruction. Cyber-attacks can be aimed directly at disrupting telecommunications services or infrastructure, or be intended to disrupt other service or industry dependent on functioning communication services. Cyber-attacks can be launched in conjunction with physical attacks in order to magnify effects or prevent effective response.

The GISP Program on Telecommunications and Cybersecurity, the Program on Information Operations, Information Assurance, and State/Enterprise Resilience (for more information on the IO Program, please **contact us**), and the Program on Law Enforcement and National Security in the Information Age (www.PLENSIA.org) are focused on understanding these threats and helping develop policies to prevent, mitigate, or respond to attacks.

Telecom and Spectrum Regulatory Policy; Management, Ownership, and Control:

Wide area networking and telecommunications are currently mediated through complex infrastructures consisting of two parallel systems, both heavily regulated. The "hard wired" infrastructure consists in the main of the remnants of the landline telephone systems and the newer cable television systems. The current "wireless" infrastructure consists of the traditional broadcast media (radio and broadcast television), satellite and the more recent wireless communication services industry.

Each of these systems is subject to different, and in many cases, inconsistent regulation and discriminatory treatment under domestic and international law. The hard-wired infrastructure was initially developed and regulated under theories of natural local monopoly and state ownership (abroad) or common carrier status (in the United States) and has recently been subjected to privatization or regulatory pressures to provide open access to private competitors.

The wireless infrastructure – essentially frequency spectrum – for broadcast was originally either allocated by government fiat (U.S.) or subject to outright government control (abroad) and content and service obligations were imposed based on a premise of spectrum scarcity. More recently, spectrum for new communication services has been allocated by auction without content or service obligations but still premised on scarcity or exclusive use. Each system – wired, wireless, and satellite – is currently subject to various domestic regulatory regimes and international treaties, and is dominated by large, capital intensive corporate organizations that compete at the periphery of their primary "traditional" business for new "data" based services.

Digitization and related technologies, however, are making all content – whether voice, text, audio or video – indistinguishable binary code, that is, "bit streams", that are transport medium indifferent. Obviously, the existing legal and regulatory system based on discriminatory treatment of different telecommunications platforms providing substantially similar services and based on geographical political boundaries that do not conform to emerging information flows or communication patterns is unstable. Thus, extant infrastructure providers are battling for market advantage by using the existing regulatory structure to try and protect their traditional businesses from competition while allowing themselves competitive entry into new services (or old services provided by others) and markets that supplant their traditional businesses.

More importantly in the long run, new developments in technology – in particular ultra-wide band and software-defined radio together with mesh networks – have the potential to make the entire existing infrastructure and regulatory regime obsolete. Indeed, they may challenge the very notion of regulation and control itself by eliminating scarcity in spectrum. Thus, determining spectrum policy is fundamental to the continued development of "cyberspace" as a platform for human communication and culture, as well as for continued economic growth and development. The two primary policy determinants in telecommunications are the related issues of allocation and governance. That is, how will spectrum (or built infrastructure) be allocated – by government fiat, free market or auction, or for free as a public good, and how will it be governed – by national or international regulation, by market or property law regulation, or as a commons. Current national developments in these areas will have significant international effects. Where there is economic, legal and regulatory instability and significant rapid technological change, as there currently is in telecommunication policy, there is need for new analysis, understanding and doctrinal developments.

The GISP Program on Telecommunications Policy examines, analyzes, and provides insight on these and related issues. **For more information, see www.global-info-society.org.**