



## 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](http://WWW.GLOBAL-INFO-SOCIETY.ORG)

### THE PROGRAM ON LAW ENFORCEMENT AND NATIONAL SECURITY IN THE INFORMATION AGE

#### Program Overview [[www.PLENSIA.org](http://www.PLENSIA.org)]

New information technologies have the potential to significantly affect how information is collected, shared, analyzed, used, or manipulated by law enforcement and national security agencies in response to certain perceived threats posed by transnational terrorism, international organized crime, cross-border criminal gangs, cybercrime, or hostile information operations directed against national or global interests. These technologies can enable remote observation or transaction monitoring (surveillance and identification), easy access to distributed data (information sharing), and efficiencies in processing and analysis (automated data and traffic analysis and data mining). In addition, the use of (and reliance on) advanced information technologies by criminals or hostile interests provides opportunities for the employ of offensive and defensive information operations to counter these threats.

The Program on Law Enforcement and National Security in the Information Age ("PLENSIA") is mainly concerned with five issues: (1) the civil liberties and privacy implications of digital law enforcement and national security practices, (2) the operational and information security aspects of such practices, (3) the opportunities for advanced information technology to improve allocation of law enforcement and security resources, (4) the offensive and defensive use of information operations, and (5) protecting against and responding to cybercrime.

#### 1. Civil liberties and privacy:

New information technologies can improve efficiencies in law enforcement and national security information collection, sharing, and analysis. Such developments, however, are challenging to political and legal systems, and social expectations, that are at least partially based on protecting certain civil liberties and individual freedoms by maintaining privacy through the "practical obscurity" of inefficient information access technologies and procedures. On the one hand there is a need to "connect the dots" through improved information sharing and analysis to provide for collective security and on the other hand the notion of individual liberty in free society is at least partially built on keeping the power to easily "connect the dots" out of the control of government agencies by maintaining or imposing inefficiencies in information sharing through a system of checks and balances, due process and technical constraints.

PLENSIA is focused on developing, examining, and articulating value sensitive development strategies that can take civil liberty and privacy concerns into account during technology development and can build in technical features that enable existing legal control mechanisms and related due process procedures for the protection of civil liberties to function. In particular, PLENSIA advocates organizational, procedural, and technical mechanisms premised on separating knowledge of behavior from knowledge of identity based on the anonymization of data (for data sharing, matching and analysis technologies) and the pseudonymization of identity (for identification and collection technologies). Technical requirements to support such strategies include rule-based processing, selective revelation, and strong credential and audit, together with appropriate architecture design.

#### 2. Operational and information security:

Information sharing among law enforcement and intelligence agencies requires maintaining operational and information security. PLENSIA is focused on organizational, procedural, and technical mechanisms to maintain such security.

See *also* the Programs on Telecommunications and Cybersecurity Policy [[www.telecom-program.org](http://www.telecom-program.org)] and on Information Operations, Information Assurance, and Resilience [[www.information-warfare.info](http://www.information-warfare.info)],

### **3. New tools for digital law enforcement and national security applications:**

Advanced collection, information sharing, and data analysis technologies, including data mining, can improve allocation of law enforcement and national security resources to more effective uses. PLENSIA examines these technologically-enabled opportunities and their affect on existing doctrine, policy, or practice.

### **4. Information operations:**

Information is an instrument of national and global power. As such, control over its use, its protection, and its manipulation, are national and global security issues. PLENSIA, together with the Program on Information Operations, Information Assurance, and Recovery/Resilience seeks to examine offensive and defensive aspects of information operations and information warfare.

### **5. Cybercrime:**

Modern technologically mediated information-based economic and social systems are also subject to cyber-attack and facilitate cybercrime.

*Cyber-attacks:* 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 business or government services or can be launched in conjunction with physical attacks in order to magnify effects or prevent effective response. Developing effective law enforcement or national security policies to deal with cyber threats is a national priority.

*Cybercrime:* The global reach of the Internet, the low marginal cost of online activity, and the relative anonymity of users have changed the balance of forces that have previously served to keep in check certain undesirable behaviors in the physical world. These characteristics of "cyberspace" have lowered the cost of perpetrating undesirable behavior by eliminating certain barriers to entry, lowering transaction costs, and reducing the probability of getting caught. In addition, these characteristics make traditional enforcement strategies, particularly identifying and apprehending perpetrators after they commit online crime, both less effective and more expensive. At the same time, however, other characteristics of cyberspace provide new opportunities to control illegal acts. Unlike in the physical world, in cyberspace certain readily identifiable third parties – Internet service providers, telecommunication providers, and victims themselves – have exclusive technical control over the infrastructure through which most illegal online behavior is carried out. These characteristics provide additional opportunities for innovative policy approaches to controlling undesirable behavior.

PLENSIA [[www.PLENSIA.org](http://www.PLENSIA.org)], the Program on Information Operations, Information Assurance, and Recovery/Resilience [[www.information-warfare.info](http://www.information-warfare.info)], and the Program on Telecommunications and Cybersecurity [[www.telecom-program.org](http://www.telecom-program.org)] are each focused on understanding aspects of these cyber-attack and cybercrime threats, and on developing policies to help prevent, mitigate, or respond to attacks.

### **PLENSIA Mission**

PLENSIA is engaged in research, publication, and outreach projects and activities on these and related issues. PLENSIA seeks to influence national and international policy- and decision-makers at every level in both the public and private sectors by providing independent research and analysis, sound advice and insight, and a forum for objective analysis and discourse.

**More information available at [www.global-info-society.org](http://www.global-info-society.org) and [www.PLENSIA.org](http://www.PLENSIA.org).**