1.	Record Nr.	UNINA9910255293103321
	Titolo	Cyber-Physical Security : Protecting Critical Infrastructure at the State and Local Level / / edited by Robert M. Clark, Simon Hakim
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
	ISBN	3-319-32824-7
	Edizione	[1st ed. 2017.]
	Descrizione fisica	1 online resource (XVIII, 281 p. 32 illus. in color.)
	Collana	Protecting Critical Infrastructure ; ; 3
	Disciplina	320
	Soggetti	Political science Water pollution Transportation Political Science Waste Water Technology / Water Pollution Control / Water Management / Aquatic Pollution
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di bibliografia	Includes bibliographical references at the end of each chapters.
	Nota di contenuto	Protecting Critical Infrastructure at the State Provincial and Local Level: Issues in Cyber-Physical Security -- Cybersecurity Terminology and Frameworks -- Assessing Cyber Threats and Solutions for Municipalities -- Cyber Perimeters for Critical Infrastructures -- A Security Evaluation of a Municipal Computer Network: The Case of Collaboration between the City of Pittsburgh and Carnegie Mellon University -- Cyber Risks in the Marine Transportation System -- Creating a Cybersecurity Culture for Your Water/Waste Water Utility -- The Community Cyber Security Maturity Model -- Fighting Cybercrime: A Joint Effort -- Cybersecurity Challenges: The Israeli Water Sector Example -- Efforts to Get People Involved In Cyber-Physical Security: Case Studies of Australia And Singapore -- Cyber Security, Trust-Building and Trust-Management: As Tools for Multi-Agency Cooperation within the Functions Vital To Society An Analysis of the Nature of Spam as Cybercrime -- Securing the Automotive Critical Infrastructure.
	Sommario/riassunto	This book focuses on the vulnerabilities of state and local services to cyber-threats and suggests possible protective action that might be

taken against such threats. Cyber-threats to U.S. critical infrastructure are of growing concern to policymakers, managers and consumers. Information and communications technology (ICT) is ubiquitous and many ICT devices and other components are interdependent; therefore, disruption of one component may have a negative, cascading effect on others. Cyber-attacks might include denial of service, theft or manipulation of data. Damage to critical infrastructure through a cyber-based attack could have a significant impact on the national security, the economy, and the livelihood and safety of many individual citizens. Traditionally cyber security has generally been viewed as being focused on higher level threats such as those against the internet or the Federal government. Little attention has been paid to cyber-security at the state and local level. However, these governmental units play a critical role in providing services to local residents and consequently are highly vulnerable to cyber-threats. The failure of these services, such as waste water collection and water supply, transportation, public safety, utility services, and communication services, would pose a great threat to the public. Featuring contributions from leading experts in the field, this volume is intended for state and local government officials and managers, state and Federal officials, academics, and public policy specialists.