This article identifies ethical and management challenges facing public managers and speculates about what the consequences may be for the public when government agencies in the United States go on line (i.e., access the Internet and establish Web sites). The article is organized into five sections. The first section discusses the meaning of cyber management as a prelude to developing organizational strategies for promoting Internet use and discouraging Internet abuse. Section 2 draws the reader’s attention to the specific content of acceptable use policies for the Internet. Section 3 then explores the challenges facing public managers to understand and abate the undesirable and sometimes unethical consequences that Internet usage may have for social or group life in public organizations. This discussion is followed by an examination of government use and abuse of the Internet. The final section highlights questions that must be answered in order for public managers to become effective cyber-age managers.
information retrieval and dissemination. Indeed, a new occupational specialty has been created for just this purpose—the Webmaster. Nearly every organization, except perhaps those that have outsourced their Internet services, has a Webmaster. This person is expected to know the technical ins and outs of creating and maintaining sites (sometimes referred to as home pages) on the World Wide Web. Moreover, he or she must monitor traffic through the site and make sure that the Web server hardware and software are operating properly. The Webmaster is also likely to know how to write common gateway interface scripts using computer languages such as Java, Perl, C++, and others.

A Webmaster could be considered a cyber manager but cyber management encompasses much more. The more has to do with understanding and dealing with the internal and external dynamics of the rapidly expanding use of information technologies, especially Internet-based technologies, in public organizations. Those dynamics include possible changes in how employees relate to one another and their organizational superiors, and how the organization itself may experience horizontal and vertical shifts in communication and authority patterns. Traditional top-down management styles, for example, may not be particularly effective in cyber workplaces. Nor may traditional authority patterns based on the organizational hierarchy retain as much meaning or presence in cyber-driven organizations.

The organizational imperative—that is, to get ahead one must swear allegiance and fealty to the company line—is likely to become blurred and pushed aside in favor of a more open, participative, and even a democratic workplace. As Sclove (1995, 232) maintains, "personal computers and telecommunications harbor the potential for allowing more democratic, decentralized, and debureaucratized social coordination, but much remains to be learned about effective strategies for realizing that potential." Sclove is correct. There is much to learn. Current efforts to apply effective strategies for debureaucratizing organizations, public and private, are mostly trial-and-error experiences.

Similarly, very little is known or understood about what might be the ethical or unethical implications of this brave new world. Effective cyber managers must be able to anticipate and respond to new ethical issues and challenges wrought by the information revolution. But what are some of these issues? And, what can or should managers do to resolve them? One issue is Internet use and—abuse.

When an agency decides to go online to establish a Web site and access the Internet—among the very first decisions that must be made is: "Who in the organization should be granted access privileges?" This question is usually followed by: "Who needs access and who doesn't?" And the third question is: "How might the privilege be abused?" Might there be undesirable if not unethical use of the Internet? The answer to this last question is clearly yes. But, what constitutes abuse and what might be clone to discourage it? Consider the following behaviors: surfing the Web for entertainment; downloading or viewing obscene or sexually oriented material; advertising or soliciting for personal financial gain; making political statements or promoting candidates for public office; posting or downloading derogatory racial, ethnic, or religious material; wagering, betting, or selling chances; using pseudonyms or pen names when transmitting electronic messages. Most public managers would probably regard these behaviors as undesirable, if not unethical, and perhaps even illegal. Thus there is likely to be considerable incentive to put rules or policies into place that prevent such behaviors and punish those who violate the rules.

Putting an acceptable use policy for the Internet in place, however, can be a tricky matter if it detracts from the presumed benefits of accessing the Internet in the first place. For example, many public managers believe that access to the Internet can stimulate and empower employees. This change can, in turn, result in more innovative and responsive government. Thus there is a substantial incentive to support employees’ access to and experimentation with the vast storehouse of data and information on the World Wide Web, electronic bulletin boards, listservs, and chat rooms. Finding the balance point between Internet use and abuse is, however, a major challenge for public managers.

Nonetheless, the challenge must be met and many government managers are attempting to do so, although not all acknowledge the potential for abuse. Some government officials believe that once the novelty of the Internet diminishes there will be little to worry about. After all, one might argue, the Internet is really like any other new information technology such as the telephone, fax machine, and the copy machine. In time, it will be treated as a routine part of the workplace.

Finding the balance point for many public managers means developing, implementing, and enforcing an acceptable use policy for the Internet. But what are the key components of such a policy? How and why do the components vary from organization to organization?

Acceptable Use Policies for the Internet

What have public agencies done to prevent Internet abuse
and yet encourage Internet use? To answer this question, a survey was conducted in the spring of 1997 of state and local government agencies with Web sites. The tracking study cited earlier contains information on the electronic mail addresses of the Webmasters at many state sites. Thus a number of agencies could be contacted to retrieve information about their acceptable use policies. Additionally, the author used the Web to locate government sites and communicate directly with many Webmasters. In total, over 60 acceptable use policies were retrieved from special districts, cities, counties, and 34 state agencies in 31 states. (See Appendix A for a list of government organizations that have put their policies online.) These policies do not constitute a random sample, but they do provide first-cut information about these important policies and emerging practices in government.

What do these policies emphasize? How comprehensive are they? What kind of guidance do they give? Before these questions are addressed, it may be helpful to identify the kinds of Internet usage that a public employee might pursue. There are four primary categories of Internet usage: sending and receiving electronic mail (known as e-mail), accessing and posting documents on the World Wide Web, sending and retrieving computer files (known as file transfer protocol or FTP), and joining electronic discussion groups (such as news groups, listservs, and Internet relay chat groups). E-mail is the most widely used Internet service, although many users are active in all categories.

A review of the acceptable use policies indicates that most place some type of restriction on who can access the Internet. This is usually couched in terms of "need" or job relevance. Accounts and passwords must be requested by a user and approved by a higher authority. Open access, giving nearly anyone in the organization an account, is uncommon. The village of Downers Grove, Illinois, is one exception. Its two-page acceptable use policy offers employees trial subscriptions to the Internet. Employees may use the account for three months at no cost but are required to contribute three dollars per pay period once their trial subscription expires.

It is also uncommon for public organizations to allow employees to use Internet accounts for personal purposes. The vast majority of public organizations among those surveyed limit Internet use in official business. There are, however, some exceptions. Washington County, Minnesota, for example, allows its employees to use computers, networks, and electronic mail for "incidental and occasional personal business use" provided that such use is (1) done on the employee's personal time, (2) does not interfere with the employee's or other employees' job activities, and (3) does not result in incremental expense for the county. The state of Oregon has a similar policy which states that "limited personal uses are allowed." Such use must be "at virtually no cost to the state" and "be trivial compared to use for assigned work." The state of Washington also permits employees limited personal use of state resources (e.g., local telephone calls and Internet messages) so long as it does not result in additional costs to the state. Another state agency, the New York State Office of Real Property Services, has deliberately refrained from prohibiting personal use of the Internet because "we want to get folks thinking about how they can use it to do their jobs better" (message posted on the GOVPUB listserv by Fran Pinto, Internet Coordinator, September 6, 1996).

Nearly every acceptable use policy for the Internet contains a statement of purpose, although most use generic language like "to advance the mission" of the city, county, or state or "for conducting official state business." The New Jersey policy asserts that the state's public presence on the Internet presents opportunities to improve communications and public service, extend government service hours, and enhance the image of government.

Perhaps the most thoughtful statement of purpose among the acceptable use policies reviewed for this article is contained in the acceptable use policy of the city of Fort Collins, Colorado. According to Fort Collins's document, the dissemination of information over the Internet is expected (1) to contribute to the economic development of the city by providing favorable information via the World Wide Web to current and potential visitors and residents, (2) to aid in policy development and decision making by giving employees immediate access to research material and other technical and professional information, (3) to conserve resources that would otherwise be consumed by the use of paper and fossil fuels and by employee attendance at conferences, (4) to foster participatory democracy by encouraging citizen involvement in and understanding of local issues, and (5) to improve service delivery by promoting and facilitating efficiency and innovation.

Regarding the use and abuse of Internet privileges, the policy documents reviewed here generally reflect one of three approaches. The most generic approach is to remind the user that the Internet is no different from any other information technology (telephone, fax machine, copying machine, etc.) and the user is subject to the same ethical and legal standards. There may also be a brief enumeration of forbidden behaviors such as "don't harass or threaten" anyone. Some agencies cite city or county ordinances or state statutes regarding the illegal uses of communication technologies.
A second approach is to develop a more detailed statement of acceptable and unacceptable behaviors. This approach might be labeled formalistic. The California Housing Finance Agency is an example. The agency lists the following as acceptable activities:

- General communications with state, federal, or local government personnel, vendors, contractors, consultants or other business partners on bona fide agency business matters.
- Electronic mail with business associates outside the agency on matters that directly relate to the user’s job duties.
- World Wide Web access for bona fide agency-related and specific job-related reasons.

Unacceptable activities, those that do not conform to the purpose, goals, and mission of the agency include:

- Activities for private or personal profit, for example: consulting for pay, selling goods for companies such as Avon and Amway, and providing tax preparation services.
- Use for personal gain in any form.
- Access to Web sites that have no direct relevance to agency business (e.g., sports scores, games, hobbies, etc.).
- Use for any illegal purpose.
- The transmission of threatening, obscene, or harassing messages or the use of inappropriate language for which the agency could be held liable.
- The access or downloading of obscene, sexually explicit, or tasteless and offensive materials in any form including multimedia photos, video, or audio.
- The downloading of software or data without authorization.
- Excessive use of e-mail for personal communication or any purpose not related to business.
- The intentional seeking of information about others unless expressly authorized to do so in writing. This includes obtaining copies of such information, modifying data, and obtaining passwords.
- Interference with or disrupting network operations including the distribution of unsolicited advertising, propagation of computer viruses, or using the network to gain unauthorized entry to another computer.
- The divulging of passwords, phone numbers, or other network access information to any unauthorized persons.

The formalistic approach typically requires the user to sign a statement that he or she has read, understands, and agrees to abide by the agency’s acceptable use policy. Failure to abide by the policy can result in disciplinary action including, but not limited to, termination of access privileges or, in serious cases, termination of employment.

A third approach can be labeled a guidelines approach. This type of acceptable use policy is long on guidelines, brief on dos and don’ts, and comes across as nonpunitive. One example is the policy of the Greene County, Ohio, library. The Greene County policy informs the user that he or she must use the Internet in a responsible, efficient, ethical, and legal manner. It then proceeds to describe acceptable and unacceptable uses. Finally, two pages are devoted to describing online etiquette.

The adoption of an acceptable use policy by a public organization may constitute an important first step in discouraging the more overt forms of undesirable behavior in the workplace; however, more subtle yet equally important changes may take place in the agency’s group life as a result of going online. The next section examines several of these possible changes.

The Interact and Group Life in the Workplace

The technical aspects of accessing the Internet, while challenging, may pale alongside the challenge faced by managers to understand and prevent the undesirable and sometimes unethical consequences that the use of this technology may have on social or group life in public agencies. For example, a study by Markus (1994, 119) on the effects of e-mail on social life in the corporate workplace found that negative effects, such as making the workplace less personal, were a product of two factors—the technology itself (e.g., the depersonalization of social relations due to a reduction in the need for face-to-face interaction) and choices by users or employees “to avoid unwanted social interactions.” In other words, e-mail technology itself is not solely responsible for “negative” social effects in the workplace. Employees can and do make choices about who they want to communicate with and who they do not. Managers committed to promoting a strong ethical climate in their organizations are likely to find this type of situation especially challenging, particularly in light of the nearly total lack of knowledge of such behavior.

Another example of a possibly undesirable outcome of
information-sharing technology in the workplace is provided by Orlikowski’s (1997) study of the introduction of groupware (Lotus Notes) into one office of a large corporation. She was interested in finding out how this technology with its emphasis on information sharing and cooperation would be received. Would it, she asked, act as a “counterculture to an organization’s structural properties (competitive and individualistic culture, rigid hierarchy)?” (Kling, 1997, 174). Orlikowski found that top-level managers and front-line employees were not reluctant to share information that presumably benefited the company at large. However, this spirit of teamwork and sharing did not extend to mid-career managers, who believed that by sharing their knowledge with others they would lose a competitive advantage over their peers. In other words, information ownership was viewed by mid-career professionals as an essential ingredient in advancing their careers. Under these circumstances, why would one want to use information-sharing technology to its fullest extent? It would be contrary to the individual’s self-interest to do so. Although Orlikowski’s study was exploratory, it certainly suggests a downside to information-sharing technologies (electronic mail, listservs, and bulletin boards.) Even if an agency establishes an Intranet (an internal information technology that uses Internet protocols and is accessible by members of the organization), it cannot be assumed that information will be widely shared or free flowing.

There are other consequences for an organization’s group life as a result of going online. On the negative side, a diminished ethical environment could result if the “frontier” character of the Internet with its stress on individualism and the depersonalization of relationships encourages employees to engage each other and the agency’s clientele in a manner that deems human dignity and diminishes respect for others. Several studies of online behavior suggest that some users are more direct, and even abrasive with others in the absence of face-to-face exchanges (Kiesler, Siegel, and McGuire, 1984). Are employees likely to treat each other or the public differently, perhaps rudely? This is an empirical question that can and should be answered.

On the positive side, the ethical environment of the workplace could be enhanced if electronic communication enabled members of the organization to obtain greater knowledge of the internal and external workings of the organization and therefore a better understanding of their own role in and contribution to the success of the agency. Insofar as members of an organization are able to reach out to peers in other organizations throughout the nation and world, they are likely to obtain an even broader understanding of their work.

The complexity of modern organizations often results in a tunnel vision that can lead to confusion, apathy, and even alienation on the part of some employees—circumstances hardly consistent with a strong ethical workplace. Internet usage may enable employees to sort through complexity and therefore become more productive and ethical. Indeed, there is some limited evidence supporting this proposition. In a study of municipal employees’ use of electronic mail, it was found that greater e-mail use resulted in employees’ becoming more committed to their employer and developing a stronger bond with their city government (Huff, Sproull, and Kiesler, 1989). This finding is especially suggestive because the study compared computer communication with more traditional forms of communication—telephone exchanges and written memos—and found no relationship between employee commitment to the organization and the extent to which the employee communicated with others via telephone or written memorandum.

Government Use and Abuse of the Internet

Other ethical and perhaps legal challenges go beyond employee access and use of the Internet and have to do with the posture of government itself. Presumably in a democracy, online governments and their leaders should promote democratic practices such as easier and greater citizen access to public information while at the same time preventing the disclosure of sensitive information stored in governmental data bases. It is one thing to post information about neighborhood crime rates or AIDS statistics and another to allow public access to names or addresses of victims. Likewise, the question might be asked: Is a public service being provided when a property appraiser’s office creates a searchable data base containing the names and addresses of owners and the property values of residential and commercial real estate? Or is this merely making it easier for scam artists, thieves, and other criminals to employ the same technology to target would-be victims?

The possibility of the misuse of government data bases raises the very important issue of how to prevent it. Consider the case of drivers license and automobile registration in Texas. This information has been public for some time and has been drawn upon primarily by insurance companies, private investigators, and even family members looking for missing relatives. Recently, a private firm in Dallas placed drivers license and automobile registration information in a searchable data base on the Internet (http://www.publiclink.com/). This site enables anyone who possesses a Texas drivers license, owns a personal computer, and has an Internet connection to look up any other Texan and any Texas license plate number. The site developers inform visitors that the data base will
be expanded in the future. Is it likely that an expanded 
data base might include information about arrest and 
conviction records, marriage records, or voter registration?

Many governments are also facing tight budgets and could 
be motivated to be entrepreneurial by selling advertising 
space on their official home pages or charging for 
hypertext links to business firms. Very entrepreneurial 
governments might even go so far as to endorse a product 
as the “official” product of its city, county, or state! Would 
these practices be ethical? Legal? Is the endorsement of a 
product or charging for Web links any different from 
placing commercial ads on municipally owned buses or 
city subways? The commercialization of the Internet is, of 
course, well underway. But how far should we go in 
commercializing government?

Finally, there is the matter of electronic communication 
between public officials (elected and appointed) and 
citizens. Few (small d) democrats would object to e-mail 
replacing fax messages between citizens and public 
officials, but it may be an entirely different matter when the 
communication path is between officeholders or between 
public employees and their elected bosses. Although some 
small communities such as Downers Grove, Illinois, 
encourage employees who hold Internet accounts to 
“communicate information to elected officials, as needed,” 
this position is more likely to be the exception than the 
rule. Direct electronic communication between elected 
officials in the same city, county, or state government, 
especially if it deals with the public’s business, may 
dermine the public’s preference for government in the 
sunshine. Will the information (r)age, especially in its 
electronic form, cast a cloud over government in the 
sunshine? Or, will public officials exercise due care, 
diligence, and caution before jumping on the keyboard and 
sending important messages to elected peers or top 
managers in their government?

Questions and Some Answers

This article raises many questions that need to be 
answered if public managers are going to be able to meet 
the growing and formidable management and ethical 
challenges of the cyber age. This section, therefore, 
attempts to draw together a number of questions raised 
above and puts forward some answers in the form of 
hypotheses.

Going Online

Why are so many public organizations in the United States 
going online? And why are some agencies going online 
faster than others? While the answer to the first question 
might appear straightforward—to improve service delivery, 
disseminate information, and increase organizational 
responsiveness—there may be other less obvious reasons. 
Studies of the diffusion of social and technological 
innovations conducted in many fields suggest that the 
adopter of an innovation such as setting up a Web site 
can be a result of many factors. For example, it may be 
that larger, more affluent, and professionally oriented 
agencies are more likely to go online faster than smaller, 
less affluent, and less professionally oriented agencies. It 
may also be the case that there is a cuing effect. That is, 
smaller agencies may be taking cues from larger agencies 
that have already developed a Web site. Additionally, the 
rapid rate of the adoption and use of Internet technology 
by federal agencies may have spurred state and local 
government agencies to do the same. Finally, there is 
always the possibility that professional competition to be 
on the leading edge of technology motivates some 
adopters to take action faster than other adopters.

Managing Behavior with Acceptable Use Policies

Are public employees abusing their Internet privileges? 
Moreover, insofar as abuse occurs, how serious is it? And, 
what are the consequences for their organization? The 
public? Is it costly to their organization in terms of lost 
productivity or diminished service quality? Does Internet 
abuse diminish the ethical environment of an agency? 
These questions can and should be answered by careful, 
systematic empirical research. At the moment, however, 
one can only speculate about what might be happening, 
although a few abuse stories (mostly dealing with business 
firms) have been reported in the popular press.

How are acceptable use policies working out? Are they 
making a positive difference? If not, why not? Do 
acceptable use policies foster a strong ethical 
environment, or are they largely innocuous? Moreover, do 
some acceptable use policies stifle employee creativity 
and problem solving effectiveness? It is most likely that the 
policy developed by an organization will mirror the 
prevailing values or culture of the organization. In other 
words, a heavily rule-oriented organization is likely to put 
together a heavily rule-oriented acceptable use policy. 
Similarly, an organization that is more trusting, (i.e., where 
employees are accorded greater discretion, trust, and 
respect) is more likely to develop an acceptable use policy 
that relies on self-policing to promote acceptable (and 
hopefully ethical) Internet behaviors and discourage 
unethical acts.

It is, of course, possible that the Internet is sufficiently 
different from other workplace technologies to require 
prevailing management practices, including the 
organization’s culture itself, to change significantly in order 
to accommodate new ways of doing things. Consider the

Group Life in the Workplace

Earlier it was noted that some research shows that electronic communication can have negative consequences for group life in an organization. That is, employees can use e-mail to engage in selective communication with other members of the organization. Thus, it is conceivable that instead of facilitating communication and encouraging team work, the technology may foster just the opposite. It is also possible to imagine a workplace that is less civil and ethical insofar as employees treat each other with less respect and consideration.

On the other hand, could the reverse occur? Might the ethical environment of a public organization actually be strengthened when its government goes online? It could be hypothesized that the ethical environment will be strengthened because as organizational members access and use the Internet, they will become more trusting and respectful of others, including their organizational superiors. This could occur because information would become less scarce and would therefore reduce status differences between employees and managers. The flattening of the status or authority structure could motivate workers and managers to treat each other with greater respect and could engender trust. Previous research has shown that high levels of organizational trust and respect go hand in hand with a strong ethical environment (Menzel, 1993; 1996).

Group life in the workplace might also be altered if Internet access and use fosters the democratization of information and communication. Widespread use of the Internet could result in a more democratic workplace—one in which employees feel a sense of participation, ownership, empowerment, and self-management. Could the idea and ideal of a democratic workplace be realized?

Government (Mis)use of the Internet

Are government agencies opening their data banks too quickly and too widely? What safeguards are in place to prevent government data from being used improperly by private-sector organizations? Are public agencies becoming too entrepreneurial with regard to selling government data or charging business firms for links placed on an agency’s home page? Is the Internet a catalyst for the commercialization of government? If so, are there undesirable side effects? For example, a municipality that charges local businesses for links to the city’s home page could put itself at a competitive disadvantage with other cities that provide this service free of charge.

Given the exploratory nature of this article, the most appropriate conclusion is to challenge future investigators to pursue some of the leads highlighted in the previous pages. It seems abundantly evident that there is a substantial need for systematic study of the interplay between Internet use and organizational behavior and performance. Indeed serious work in this area is in its infancy. As Kling (1996, 53) poignantly remarks about organizational worklife: “There is little research that examines the relationships between work online and life in the organization off line.” “We need,” he concludes, “a strong research program that examines how the social design/organization of electronic forums strengthens or weakens group life in workplaces and communities.” The time to begin this important work is at hand.

Acknowledgement

The author would like to acknowledge the constructive reviews of this paper by two unknown referees and Professors Evan Berman of the University of Central Florida, James S. Bowman of Florida State University, Monty Van Wart of Iowa State University, and Jonathan West of the University of Miami. Thanks are also due to Stephen J. Bonczek, Managing Director of the City of Reading, Pennsylvania, and Thomas J. Bonfield, City Manager of Temple Terrace, Florida, for providing helpful comments and criticism. Jonathan Lewis and Jennifer Codo, MPA students at the University of South Florida, provided valuable research assistance. All errors of omission and commission rest solely with the author.

References


Appendix 1

Government Web Sites with Acceptable Use Policies and Documents On Line

Alabama
AL Research and Education Network
www.asc.edu/html/accusepol.html

Alaska
urunw.gov.state.ak.us/ltgov/tic/offhtml.html Dept. of Environmental Conservation
www.state.ak.us/localallakpages/ENV CONSERV/das/is/webcord/interpol.htm

Arizona
www.state.az.us/isd/forms/inetagre.htm

California
Department of Information Technology
www.doit.ca.gov/simm/internet.asp

Connecticut
www.state.ct.us/cmac/statpoli.htm

Delaware
www.otm.state.de.us/otm/sitnlaw.htm

Indiana
www.state.in.us/dpoc/dpoc.html

Kansas
www.ink.org/public/itask/policy/policy.htm

Kentucky
www.state.ky.us/kirm/docs.htm

Louisiana
www.doa.state.la.us/otm/accept.htm

Maine
www.state.me.us/ispb/interpol.htm

Minnesota
www.state.mn.us/ebranch/admin/ipo/hb/document/seltop.1.html#table or www.state.mn.us/ebranch/admin/internet-usage.html

Missouri
www.state.mo.us/comofc/i_policy.htm

Nebraska
www.das.state.ne.us/das_doc/doc/aup.htm

New Jersey
www.state.nj.us/infobank/circular/cir9701s.htm

New York
www.irm.state.ny.us/policy/tp_968.htm

North Carolina
www.osc.state.nc.us/irmc/documents/approvals/irmcinet.html

North Dakota
www.state.nd.us/isd/external.html

Ohio
www.state.oh.us/das/direct/97-23.html or www.ohio.gov/opp/opp-pol.htm

Oregon

www.state.or.us/IRMD/policies/03-13net.htm or
www.state.or.us/IRMD/policies.htm

Seattle, Washington

www.ci.seattle.wa.us/pan/iau5-2.htm

South Carolina

www.state.sc.us/nis_itg/em_guidelines.html or
www.state.sc.us/nis_itg/index.html

South Dakota

www.state.sd.us/bit/is/document/internet.htm

Tennessee

www.state.tn.us.finance/oir/int-aup.html

Texas

State Lib. and Archives Com.
www.tsl.state.tx.us/IRT/netpol_rev3.htm

U.S. Department of Agriculture National Agricultural Library

www.nal.usda.gov/general_info/webpolicy.html

Utah

www.gvnfo.state.ut.us/sitc/aup.htm

Washington

www.wa.gov/dis/tsd/tutorial/policy.htm

Donald C. Menzel is professor of public administration and director of the Division of Public Administration at Northern Illinois University. He is a former member of the faculties at the University of South Florida and West Virginia University. He is currently working on a book Ethics Management in Government and conducting research on the ethical environment of public administration graduate education.