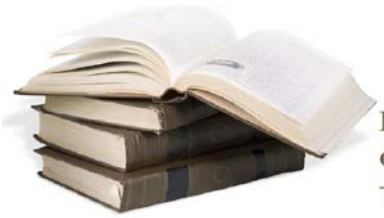

Encyclopedic Dictionary
of Public Administration
The reference for understanding government action

CYBER-SURVEILLANCE

Monica Tremblay, Professional researcher
École nationale d'administration publique
monica.tremblay@enap.ca

Cyber-surveillance is a mechanism for the surveillance of persons, objects or processes that is based on new technologies and that is operated from and on data networks, such as the Internet. Its purpose is to facilitate surveillance, in keeping with the quantity, rapidity or complexity of the data to be processed. As with surveillance as a whole, it refers to the gathering and analysis of information in the pursuit of various finalities – in particular, preventing certain risks, orienting human behaviours and, in the event of a problem, locating the persons responsible (Commission de l'éthique de la science et de la technologie, 2008; Cahen, n.d.; Boudreau, 2006).

"Cyber-surveillance" is part of a category of recent terms coined following the advent of cybernetics in 1948 and whose use has become increasingly widespread since the dawning of electronic communication networks in the 1970s. Many new words came into circulation especially as access to the Internet became generalized in the mid-1990s. All in all, the prefix "cyber-" has been linked to activities that are not new in themselves but that are now performed in virtual space using computer systems and telecommunications.

Cyber-surveillance has, over time, become a part of our daily lives, as the ongoing development, spread and refinement of information technologies have expanded the capabilities for managing countless risks and ensuring the security of persons, places, data, infrastructures and processes across a range of sectors (Commission nationale de l'informatique et des libertés, 2004; Leman-Langlois and Ouimet, 2006; Bajc, 2007). Subsequent to international terrorist attacks, such as those perpetrated in the United States on September 11, 2001 or in the London Underground in July 2005, recourse to cyber-surveillance has intensified, driven by the need to implement measures to reduce not only threats to the security of States and their populations but also the fears that such threats have given rise to.

Elsewhere, cyber-surveillance has been increasingly relied on by governments to carry out certain administrative tasks in the health, welfare, education and civil security sectors (Commission de l'éthique de la science et de la technologie, 2008). Businesses keen to protect certain information or to monitor the behaviour of their employees or clients have also engaged in "cyberveillance" and corporate surveillance. Civil society and citizens' organizations may also use information technologies to monitor the words and deeds of authorities or businesses as part of strategies to publicly denounce conduct they deem to be unacceptable (Häyhtiö and Rinne, 2009; Leman-Langlois and Ouimet, 2006; Boudreau, 2006). Finally, delinquents and criminal groups may turn to cyber-surveillance in the pursuit of their objectives.

Cyber-surveillance involves the gathering of data by means of technological tools and surveillance software programs. This often abundant data (consisting in or relating to events, messages, movements, system access, etc.) is recorded and then sifted through by automated surveillance computers. The enhanced data resulting from this filtering process can then be used by human investigators who contribute to decisions about the best courses of action to adopt. It has thus become possible to monitor the behaviours of individuals in real time, over a specific period and around the world (Bajc, 2007). One common example of cyber-surveillance consists in the interception and analysis of electronic messages (Cahen, n.d.; Commission nationale de l'informatique et des libertés, 2004). On an international scale, ECHELON refers to an electronic espionage project launched by five signatory countries that was designed and coordinated by the US National Security Agency and whose existence was disclosed in 1988. This signals intelligence collection system enables the participating governments to intercept and inspect the electronic and non-electronic telecommunications carried over various global networks. Powerful computers are used to analyze a phenomenal quantity of data gathered by various systems for the purpose of filtering out those messages containing potentially strategic information – in particular of a kind relating to a national security threat. There are numerous examples of government-run cyber-surveillance operations, particularly as part of efforts to counter identity theft, computer intrusion, terrorism, business fraud or pedophilia. Cyber-surveillance is a tool permitting mass surveillance.

Depending on the goal being pursued, cyber-surveillance practices can be of varying complexity, with mass surveillance being generally cited as one of the most advanced. The more the data to be collected and processed is abundant and the more the variables to be accounted for are strategically important, the more a given surveillance system will have to be sophisticated.

Cyber-surveillance can serve a variety of purposes: preventing or pre-empting a variety of threats; detecting various crime or offence risks; or conducting investigations in the aftermath of an event. “Cyber-surveillance can be useful not only in terms of the security or sound management of a data system but also in terms of monitoring the appropriate transmission of correspondence” (Cahen, n.d., p. 1).

Though technological advances have created a potential for undreamed-of surveillance practices, cyber-surveillance itself has also aroused questions and fears. Increasingly omnipresent and invisible, often performed remotely and without the knowledge of the individuals concerned, cyber-surveillance has fanned fears of a form of tight social control, exerted by authorities having the ability to ultimately repress any individual freedom. Concerns have also been voiced as to the risk of seeing the finalities for which data were initially gathered being diverted toward purposes that are detrimental to the privacy and integrity of individuals (Boudreau, 2010). In the same vein, the risks of racial profiling and discrimination have become a matter of serious concern (Biseul, 2004). Questions also crop up over how to achieve or maintain a balance between the quest for security and respect for human rights. To what extent will it be possible to invoke reasons of State security when gathering and cross-checking information against other personal data without also causing prejudice to privacy? Technology has now made it possible to perform mass surveillance, such that official suspects are not the only ones whose activities are subject to scrutiny; anyone who happens to find him- or herself monitored under a surveillance process becomes a de facto suspect for those who are watching (Commission nationale de l'informatique et des libertés, 2004; Commission de l'éthique de la science et de la technologie, 2008). Air passenger surveillance constitutes but one example of this trend. In the context of globalization, particular attention should be dedicated to the legal and ethical issues surrounding the sharing and use of data gathered under a given legislative regime.

Bibliography

Bajc, V. (2007). "Debating Surveillance in the Age of Security," *American Behavioral Scientist*, vol. 50, no. 12, pp. 1567-1591.

Biseul, X. (2004). *Cybersurveillance : les nouvelles technologies ravivent les vieilles peurs*, www.01net.com/article/248848.html (last retrieved in April 2010).

Commission nationale de l'informatique et des libertés (2004). *La cybersurveillance sur les lieux de travail*, www.cnil.fr/fileadmin/documents/approfondir/dossier/travail/cyber_conclusions.pdf (last retrieved in April 2010).

Boudreau, C. (2010). *Cybercriminalité et cybersurveillance*, lecture notes, ENAP.

Boudreau, C. (2006). "Multipolarité de la surveillance et gestion des médicaments au Québec," *Recherches sociographiques*, vol. 47, no. 2, pp. 299-320.

Cahen, M. (n. d.). *Le rôle de l'administrateur réseau dans la cybersurveillance*, www.netalya.com/fr/Article2.asp?CLE=162# (last retrieved in April 2010).

Commission de l'éthique de la science et de la technologie (2008). *Viser un juste équilibre : un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité*, Avis adopté à la 34e réunion de la Commission de l'éthique de la science et de la technologie le 12 février.

Häyhtiö, T. and J. Rinne (2009). "Little Brothers and Sisters Are Watching," *Information, Communication and Society*, vol. 12, no. 6, pp. 840-859.

Leman-Langlois, S. and M. Ouimet (2006). "Introduction," *Criminologie*, vol. 39, no. 1, pp. 3-6.

HOW TO CITE Tremblay, M. (2012). "Cyber-surveillance," in L. Côté and J.-F. Savard (eds.), *Encyclopedic Dictionary of Public Administration*, [online], www.dictionnaire.enap.ca

INFORMATION For further information, please visit www.dictionnaire.enap.ca

LEGAL DEPOSIT Library and Archives Canada, 2012 | ISBN 978-2-923008-70-7 (Online)