**Forum:** GA 1 – Disarmament and International Security

**Issue:** The question of cyber-surveillance on civilians

**Student Officer:** Agustin Lopez

**Position:** Former Chair



**Introduction**

Technology has become a part of everyday life. However, because of how accessible these technologies are to the public, it has become easier and more desirable for governments and other bodies to conduct surveillance, collect personal data, and intercept communications of individuals. The state, and other parties, not only can conduct targeted surveillance but they are able to organize projects of simultaneous mass surveillance, which threaten the right to privacy and the right to freedom of expression of individuals.

As technology advances and these practices become more and more common, it is of utmost importance to have clear boundaries for all parties when conducting cyber-surveillances to protect the rights of individuals. The governments that indulge in practising cyber-surveillance claim that it is for the good of the population since it can be used to investigate criminals and criminal activity, anticipate criminal activity (such as terrorist attacks), and maintain order in the country. Clear jurisdiction is needed to solve this issue, protecting the rights of citizens but also allowing the government to use cyber-surveillance.

**Definition of Key Terms**

**Cyber-surveillance**

Cyber surveillance is a term to refer to the monitoring of technological activity (such as an individual's activity on the internet) performed by governments, corporate bodies, criminal organizations or individuals (Tremblay, 2012).

**Right to privacy**

In article 12 of The Universal Declaration of Human Rights it is stated that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks”(United Nations General Assembly, 20--?, para. 20)[[1]](#footnote-0)

Furthermore, in Article 17 of the International Covenant on Civil and Political Rights, it is stated that “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation”(United Nations General Assembly, n.d., para. 53).

**Unlawful**

In point number 3 in the General Comment No.16 on Article 17 of the International Covenant on Civil and Political Rights, The Office for the High Commissioner for Human Rights states that “The term “unlawful” means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims, and objectives of the Covenant.”(Human Rights Committee, n.d., para. 3).

**General Overview**

As technology advances and it becomes more widespread, cyber-surveillance becomes more common. The question then becomes: When can the government perform cyber-surveillance? How can we protect the right of privacy of citizens that use digital platforms? How can we regulate cyber-surveillance?

**Historical Background**

Cyber-surveillance, overall, is a new issue. While surveillance has been a part of history, cyber-surveillance only started going when it became common for individuals to have access to the internet and a technological device, therefore this is a late 20th and 21st-century problem. Due to this, there have not been many attempts to solve this issue.

**Major Countries and Organizations Involved**

* **The United States of America:** Since the September 11, 2001 attacks by terrorist groups on US land, the USA has used cyber-surveillance to track down these terrorist groups. The USA also uses cyber-surveillance to investigate other crimes. It is important to note that the USA used surveillance way before the internet was created. The main organization that is allowed to conduct mass surveillance in the USA is the National Security Agency (National Security Agency Central Security Service, n.d.).
* **The Democratic People's Republic of Korea:** The state has absolute control over telecommunication and spies on the citizens. In the world report of 2013 of the Human Rights Watch, it is stated that: “North Korea operates a vast network of informants who monitor and report to the authorities fellow citizens they suspect of criminal or subversive behaviour. All media and publications are state-controlled, and unauthorized access to non-state radio or TV broadcasts is severely punished”(Human Rights Watch, 2013, para. 19).
* **The Russian Federation:** Russia has been performing mass surveillance on citizens for a long time. The Federal Service for Supervision of Communications, Information Technology and Mass Media or Roskomnadzor is responsible for censorship in telecommunications and media. According to the Human Rights Watch the government of Russia: “will gain even greater control over freedom of speech and information online when the country’s “sovereign internet” law goes into effect on November 1, 2019.”(Human Rights Watch, 2019, para. 1)
* **The People's Republic of China:** The People’s Republic of China has been performing mass surveillance on citizens; according to the Human Rights Watch: “Chinese authorities are using a mobile app to carry out illegal mass surveillance and arbitrary detention of Muslims in China’s western Xinjiang region” (Human Rights Watch, 2019, para. 1).

**Consequences**

The major consequence of cyber-surveillance is the violation of rights. First, the right to privacy can be violated by monitoring what is the activity of an individual on the internet. Furthermore, it is now common to have personal and sensitive information online which further aggravates this issue. It is important to note that cyber-surveillance can also threaten the right of expression of individuals since it can lead to censorship online or interception of messages. The interception of messages can also threaten the right of assembly and association (Article 20 of the Universal Declaration of Human Rights) as it interferes with the ability of individuals to communicate freely.

Many people question the ethical implications of cyber-surveillance since it could be considered as spying. An individual should be able to feel safe, to feel as if his private life is actually private. As human beings, it is our decision whether to share our private life or not, and cyber surveillance could be seen as a violation of the safety of the person. Matters get worse, as many countries do not explicitly say if they perform cyber-surveillance. This creates an aura of distrust from the people towards the government.

**Latest Events**

The UN Human Rights Council passed a resolution on the 27th of February of 2017 on the right to privacy in the digital age that proposes measures to protect the right of privacy of civilians while still allowing cyber-surveillance in some cases; article 2 of this resolution states: “Recalls that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality” (Human Rights Council, 2017, para. 30).

**Possible Solutions**

Most states agree that the key to solving this issue is to protect the right of privacy of individuals while still being able to perform cyber-surveillance to conduct investigations on criminal activity. There are yet to be seen any specific regulations and international norms that would establish under what situations the government could perform cyber-surveillance and in what situations it would not be allowed.

**Useful reference material**

* [Universal Declaration of Human Rights](https://www.un.org/en/universal-declaration-human-rights/)
* [International Covenant on Civil and Political Rights](https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx)
* [Human Rights Watch | Defending Human Rights Worldwide](https://www.hrw.org/)
* Report of the Office of the United Nations High Commissioner for Human Rights [The right to privacy in the digital age](https://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc)
* Human Rights Committee, General Comment 16, (Twenty-third session, 1988) [Rights Library](http://hrlibrary.umn.edu/gencomm/hrcom16.htm)
* The right to privacy in the digital age, 23 March 2017 (34/7) <https://www.right-docs.org/doc/a-hrc-res-34-7/>
* The right to privacy in the digital age, 18 December 2015 (68/166) [A/RES/69/166 - E - A/RES/69/166](https://undocs.org/A/RES/69/166)
* The right to privacy in the digital age, 18 December 2013 (68/167) [A/RES/68/167 - E - A/RES/68/167](https://undocs.org/A/RES/68/167)

**Bibliography**

Human Rights Committee. (n.d.). General Comment No.16 on Article 17 of the International Covenant on Civil and Political Rights. *University of Minnesota Rights Library.* Retrieved on March 1st 2021 from <http://hrlibrary.umn.edu/gencomm/hrcom16.htm>

Human Rights Watch. (2013).World Report 2013: North Korea. *Human Rights Watch*. Retrieved on March 1st from [https://www.hrw.org/world-report/2013/country-chapters/north-korea#](https://www.hrw.org/world-report/2013/country-chapters/north-korea)

Human Rights Watch. (2019, October 31st) .Russia: New Law Expands Government Control Online. *Human Rights Watch*. Retrieved on March 1st from <https://www.hrw.org/news/2019/10/31/russia-new-law-expands-government-control-online>

Human Rights Watch. (2019, May 2nd). How Mass Surveillance Works in Xinjiang, China. *Human Rights Watch*. Retrieved on March 2nd from <https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang>

Human Rights Council. (2017, April). The right to privacy in the digital age. *Right Docs*. Retrieved on March 2nd 2021 from <https://www.right-docs.org/doc/a-hrc-res-34-7/>

National Security Agency Central Security Service. (n.d.). *National Security Agency Central Security Service*. Retrieved on May 31st 2020 from <https://www.nsa.gov/what-we-do/signals-intelligence/>

Tremblay, M. (2012). Cyber-surveillance. *Encyclopedic Dictionary of Public Administration*. Retrieved on May 14th 2020 from [http://www.dictionnaire.enap.ca/dictionnaire/docs/definitions/definitions\_anglais/cybe](http://www.dictionnaire.enap.ca/dictionnaire/docs/definitions/definitions_anglais/cyber_surveillance.pdf)

United Nations General Assembly. (n.d.). The Universal Declaration of Human Rights. *United Nations*. Retrieved on March 1st 2021 from <https://www.un.org/en/universal-declaration-human-rights/>

United Nations General Assembly. (n.d.). International Covenant on Civil and Political Rights. *United Nations Human Rights OFficer of the High Commissioner*. Retrieved on March 1st 2021 from <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>

1. The Declaration of Human Rights was proclaimed by the United Nations General Assembly on the 10th of December of 1948. [↑](#footnote-ref-0)