Research Report

HMUN 2021

Committee: Human Rights Council

Student Officer: Myrthe Beerens and Nora Dijksta

Issue of: Ensuring civil privacy within the use of cybersecurity

Issue: Ensuring civil privacy within the use of cybersecurity
Forum: Human Rights Council
Name: Myrthe Beerens and Nora Dijkstra
Position: Chair and Deputy Chair

Introduction

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." This is Article 12 of the United Nations Universal Declaration of Human Rights. The fundamental human right of privacy is perhaps now, in the digital age, more than during any other time, under threat: private records of almost the entire world population are documented and kept in an online space. This is often used to commit crimes, such as large-scale data theft. It can, however, also be used for good: an increasing number of governments have decided to collect data from their citizens and use these to fight crime, specifically terrorist attacks. By monitoring internet activity and collecting data, governments can locate terrorists and prevent them from organizing an attack. The negative effect that comes with this, however, is that the privacy of civilians is now under threat seeing as their behavior on the internet is being monitored. Governments have more information and thus power over their citizens. This threat will be discussed in this research report.

Definition of Key Terms

Privacy

"Privacy can be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited 3 UNESCO, Global Survey on Internet Privacy and Freedom of Expression, 2012, p. 51. A/HRC/23/40 7 intervention by other uninvited individuals.4 The right to privacy is also the ability of individuals to determine who holds information about them and how is that information used." (HRC, 23rd session, agenda item 3, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue)

Cybersecurity

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

Cybercrime

Criminal acts committed using electronic communications networks and information systems or against such networks and systems.

Terrorist act

A UN panel, on March 17, 2005, described terrorism as any act "intended to cause death or serious bodily harm to civilians or non-combatants with the purpose of intimidating a population or compelling a government or an international organization to do or abstain from doing any act."

General Overview

With the rapid development of technology, numerous new methods to prevent crime have arisen. These cybersecurity methods contribute to global safety; however, they do not come without threats of their own. Cybersecurity is, among other things, often used to eliminate terrorist threats. In order to do this, governments might collect data of citizens which they can use to locate a threat. By doing this, they risk intruding on their citizens' privacy and violating the 12th article of the UN Universal Declaration of Human Rights.

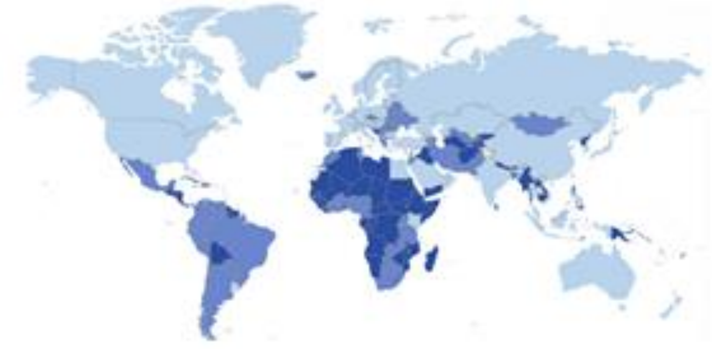
The United Nations have adopted several resolutions urging member states to join the existing organizations and protocols against terrorism. The following two clauses are from the 6th review of the UN Global Counter-Terrorism Strategy:

"19. Urges all States to respect and protect the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights 7 and article 17 of the International Covenant on Civil and Political Rights, 8 including in the context of digital communication, also while countering terrorism, in accordance with international law, in particular international human rights law, and to take measures to ensure that interferences with or restrictions on that right are not arbitrary or unlawful and are subject to effective oversight and to appropriate redress, including through judicial review or other legal means;

20. Calls upon States, while countering terrorism and preventing violent extremism conducive to terrorism, to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, by ensuring the full and effective implementation of all their obligations under international human rights law;"

As stated above, the UN has recognized the dangers the use of cyber security can entail for the right to privacy. Protecting this right, while still using cyber security effectively, is a challenge and more information and expertise on this must be gathered. This challenge is very different for countries with different levels of commitment to cybersecurity. The commitment is measured by how advanced countries are in developing their cyber security. The map below shows these levels of commitment per country, based on the Global Cybersecurity Index (GCI). The lighter the color of blue, the higher the commitment.

As shown on the map, the level of advancement of cyber security varies around the world. The higher the level of advancement, the larger the risk of violation of the citizens' right to privacy.



Disclaimer: The designations employed and the presentation of this map do not imply the expression of any opinion whatsoever on the part of the ITU concerning the legal status of any country, state, territory or area and/or of its authorities, or concerning the delimitation of its boundaries or frontiers. Efforts were made to ensure this map is free of errors however there is no warranty the map or its features are either spatially or temporally accurate or fit for a particular use. This map is provided without any warranty of any kind whatsoever, either express or implied.

Online privacy violation can fall under the next three categories: collecting personal information without notification (e.g., "cookies"), profit by selling personal information and personal information redevelopment (for example to build databases for future use and 'improve the online experience'). The first category is the most relevant when considering governments, since data might be collected to locate threats and criminals. The second category, however, might be relevant as well when considering governments might trade citizens' data for other purposes. For example: the Netherlands might have collected data on which citizens are homosexuals for certain research. For the Netherlands, outside of this research, this information would not be relevant. For a country where homosexuality is illegal, on the other hand, this information would be relevant and might be used to deny access or rights to a specific homosexual individual. This kind of incident can only be prevented when clear international rules are formulated.

Under 'Timeline of Key Events' an extensive timeline of cybercrime and government and UN responses has been provided. This should help to gain insight into the serious threat cybercrime poses to world peace and safety and governments' eagerness to eliminate this threat.

Each government makes different choices around cyber security and their citizens' privacy. For example, in China, the privacy of citizens is regarded as not as high of a priority as national safety. The concept of 'privacy' does not exist in Chinese culture the way it does in Western society. It was not until recently that the specific right to privacy was specified in decided legislation. The Chinese government collects and monitors its citizens' data in order to fight crime and ensure civil obedience.

Major Parties Involved

UNOCT

United Nations Office of Counter-Terrorism

United States of America

The USA is one of the countries with the best cyber defense in the entire world. They are also very involved in the search for solutions on this topic.

Russia

The country has a robust cybercrime black market, valued at approximately US$2 billion per year, and hosts as many as 30 highly capable cybercrime groups. Russia is also known for state-sponsored hacking.

China

Approximately 30 percent of all cyber-attacks worldwide are launched from China. The country has been accused of perpetrating state-sponsored attacks against foreign governments and businesses. China has one of the largest military groups of cyber experts in the world. China also uses the large-scale collecting and monitoring of data of citizens as a cyber security-method.

IMPACT

The International Multilateral Partnership Against Cyber-Terrorism

International Telecommunications Union (ITU)

.

The International Telecommunication Union (ITU) is the United Nations specialized agency for information and communication technologies – ICTs.

Timeline of Key Events

April 2007 Estonian government networks were harassed by unknown foreign intruders. Some government online services were temporarily disrupted and online banking was halted.

June 2007 The US Secretary of Defense's unclassified email account was hacked by unknown foreign intruders, as part of a larger series of attacks to access and exploit the Pentagon's networks.

October 2007 China's Ministry of State Security said that foreign hackers, which it claimed 42% came from Taiwan and 25% from the US, had been stealing information from Chinese key areas.

June 2008 During the presidential campaigns in the USA databases of both Republican and Democratic were hacked and downloaded by unknown foreign intruders.

January 2010 A group named the "Iranian Cyber Army" disrupted the service of the popular Chinese search engine Baidu. Users were redirected to a page showing an Iranian political message. The same "Iranian Cyber Army" had hacked into Twitter the previous December, with a similar message.

July 2011 In a speech unveiling the Department of Defense's cyber strategy, the US Deputy Secretary of Defense mentioned that a defense contractor was hacked and 24,000 files from the Department of Defense were stolen.

October 2012 The Russian firm Kaspersky discovered a worldwide cyber-attack dubbed "Red October," that had been operating since at least 2007. Hackers gathered information through vulnerabilities in Microsoft's Word and Excel programmes. The primary targets of the attack appear to be countries in Eastern Europe, the former USSR and Central Asia, although Western Europe and North America reported victims as well. The virus collected information from government embassies, research firms, military installations, energy providers, nuclear and other critical infrastructures.

June 4th 2013 In their first-ever meeting dedicated to cyber defense, NATO Defense Ministers agreed that the Alliance's cyber-defense capability should be fully operational by the autumn, extending protection to all the networks owned and operated by the Alliance.

February 2017 The UN reviewed the UN Security Council Resolution

June 15th 2017 The UNOCT (UN Office of Counter-Terrorism) was founded.

July 2nd 2018 The UN, passed a new cyber security report, which is the UN Global Counter-Terrorism Strategy

Previous attempts to resolve the issue

One of the first attempts by the UN to solve the issue was by the founding of the UNOCT (UN Office of Counter-Terrorism). The UNOCT was founded in 2017 and from that moment the UN Office had led many initiatives in order to eliminate the problem. Several initiatives are in the field of new technologies, including a project on the use of social media to gather open-source information and digital evidence to counter terrorism and violent extremism while respecting human rights. It has provided expertise in international fora on the use of unmanned aerial systems (UAS) and will develop further programming in this area.

Possible Solutions

In order to ensure the right to privacy of all world citizens are respected and protected, clear international legislation and/or UN guidelines around cyber security must be implemented. Governments are sovereign, and therefore have the right to decide where they draw the line on certain topics themselves. However, these rules or guidelines could be based on the UN definition of the right to privacy while still respecting all cultures and customs.

Appendices

- United Nations, *Universal Declaration of Human Rights,* https://www.un.org/en/universal-declaration-human-rights/
- https://undocs.org/A/RES/72/284
- https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx#:~:text=Cybersecurity%20is%20the%20collection%20of,and%20organization%20and%20user's%20assets.
- https://www.itu.int/en/ITU-D/Cybersecurity/Pages/United-Nations-Launches-Global-Cybersecurity-Index.aspx

Bibliography

- https://www.un.org/counterterrorism/cybersecurity
- https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/167/28/PDF/G1016728.pdf?OpenElement
- https://www.afcea.org/content/countries-collaborate-counter-cybercrime
- https://www.bba.org.uk/wp content/uploads/2015/02/red24+Cybercrime+Top+10+countries+where+attacks+originate+-++2015.pdf
- https://cipher.com/blog/which-country-is-1-in-cybersecurity/
- https://undocs.org/S/RES/2341(2017)
- Bigo, D., Boulet, G., Bowden, C., Carrera, S., Jeandesboz, J., & Scherrer, A. (2012). Fighting cyber crime and protecting privacy in the cloud. European Parliament http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOLLIBE_ET%282012%29462509_EN.pdf
- https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf\https://www.researchgate.net/profile/Yanfang_Wu/publication/227426731_A_comparative_study_of_online_privacy_regulations_in_the_US_and_China/links/5aa480dcaca272d448b8eec1/A-comparative-study-of-online-privacy-regulations-in-the-US-and-China.pdf