COMMITTEE :- UNITED NATIONS GENERAL ASSEMBLY - DISARMAMENT AND INTERNATIONAL SECURITY COMMITTEE (UNGA-DISEC)

AGENDA :- EVOLUTION OF SURVEILLANCE TECHNOLOGY FOR SECURITY PURPOSES

Introduction to the committee

UNGA - UNITED NATIONS GENERAL ASSEMBLY

The United Nations is an international organization founded in 1945, committed to maintaining international peace and security; developing friendly relations among nations; promoting social progress, better living standards and human rights.

The General Assembly of the United Nations occupies a central position as the chief deliberative, policymaking and representative organ of the United Nations. Composed of all 193 Members of the United Nations, it provides a unique forum for multilateral discussion of the full spectrum of international issues covered by the Charter. It is also the body from which elected countries can become the Non-Permanent members of the United Nations Security Council (UNSC).

The Assembly meets from September to December each year (main part), and thereafter, from January to September (resumed part), as required, including to take up outstanding reports from the Fourth and Fifth Committees. The Assembly is empowered to make recommendations to States on international issues within its competence. It has also initiated actions - political, economic, humanitarian, social and legal-which have benefited the lives of millions of people throughout the world.

Framing resolutions,initiating studies and making recommendations to promote international political cooperation, the development and codification of international law, the realisation of human rights and fundamental freedoms, and international collaboration in the economic, social, humanitarian, cultural, educational and health fields. Formulation of recommendations for the peaceful settlement of any situation that might impair friendly relations among countries
Likewise, to consider reports from the Security Council and other United Nations organs.

DISEC - DISARMAMENT AND INTERNATIONAL SECURITY COMMITTEE

The First Committee deals with disarmament, global challenges and threats to peace that affect the international community and seeks out solutions to the challenges in the international security regime.

It considers all disarmament and international security matters within the scope of the Charter or relating to the powers and functions of any other organ of the United Nations; the general principles of cooperation in the maintenance of international peace and security, as well as principles governing disarmament and the regulation of armaments; promotion of

cooperative arrangements and measures aimed at strengthening stability through lower levels of armaments.

The Committee works in close cooperation with the United Nations Disarmament Commission and the Geneva-based Conference on Disarmament. It is the only Main Committee of the General Assembly entitled to verbatim records coverage.

The First Committee sessions are structured into three distinctive stages:

- General debate
- Thematic discussions
- Action on drafts

It is the only Main Committee of the General Assembly entitled to verbatim records coverage pursuant to Rule 58 (a) of the rules of procedure of the General Assembly.

Introduction to the Agenda

"Disarmament Including arms control, Non-Proliferation. Prohibitions. Restrictions, Confidence building, and where needed, Elimination-Is an essential tool to secure our world and our future."

- António Guterres, United Nations Secretary-General

According to the Merriam-Webster dictionary, "close watch kept over someone or something (as by a detective)."

In relation to which we can look into, the book '1984' by English Novelist Eric Arthur Blair (George Orwell) which is "set in 1984 in Oceania, one of three perpetually warring totalitarian states (the other two are Eurasia and Eastasia). Oceania is governed by the all-controlling Party, which has brainwashed the population into unthinking obedience to its leader, Big Brother," according to the Encyclopedia Britannica.

It presents a similar case in today's world, wherein an individual's privacy and State's security is in a tussle, in the background of which we have Surveillance technologies that existed from yesterday, exist today and possibly continue to exist in the future.

Understanding Privacy Rights

Article 12 of the Universal declaration of human rights ‘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.’
The term Privacy, although in use for only a comparatively short time, actually refers to a situation which is as old as the desire of individuals to be protected from interference by others. Privacy is the individualís intimate sphere of existence which must, therefore, be concealed from the knowledge of other people and shielded from their curiosity.
Set out in those terms, one might imagine that the right was indefeasible, but we must add that it has to be reconciled with requirements relating to security, national defence and anti-terrorism campaigns. It is with a view to meeting those requirements that certain exceptions are authorised. For example, lawful interception of communications is authorised, but it is subject to compliance with stringent strict rules.

Use of surveillance for Security purposes -

Public authorities involved in the prevention and investigation of acts of terrorism and potential terrorist conspiracies have shown great interest in ensuring that the records generated by communications service providers (e.g., public and private companies providing telecommunications and Internet services) are available to them for the prevention, investigation and prosecution of serious crime, including terrorism.

An accompanying source of privacy related concern has been the growing practice of some intelligence agencies to gather bulk information about their citizens using telephone and Internet networks as part of their counter-terrorism efforts (Council of Europe, Parliamentary

Assembly, 2015(b), paras. 1-3). Such bulk information usually contains descriptive information about other data and is called 'metadata' (Council of Europe, Parliamentary Assembly, 2015(a), para. 18). An example of metadata is the Internet Protocol address associated with a computer from which an individual had sent an email (Council of Europe, Parliamentary Assembly, 2015(b), para.12). Other examples are a list of telephone numbers which an individual dialled on a particular day, or a list of websites which an individual has visited.

The fact that the causes of terrorism include psychological and sociological factors provide a partial explanation as to why intelligence services are often keen to collect metadata as part of their efforts to identify terrorist networks.

Use of surveillance for Public Health purpose -

According to the World Health Organization (WHO), Public health surveillance is the continuous, systematic collection, analysis and interpretation of health-related data.

Disease surveillance data :

- serves as an early warning system for impending outbreaks that could become public health emergencies;

- enables monitoring and evaluation of the impact of an intervention, helps track progress towards specific goals;

- and monitors and clarifies the epidemiology of health problems, guiding priority-setting and planning and evaluation public health policy and strategies.

Humanitarian emergencies increase the risk of transmission of infectious diseases and other health conditions such as severe malnutrition. An effective disease surveillance system is essential to detecting disease outbreaks quickly before they spread, cost lives and become difficult to control. Effective surveillance can improve disease outbreak detection in emergency settings, such as in countries in conflict or following a natural disaster.

The WHO's 'The Surveillance System on Attacks on Healthcare (SSA)', is a global standardised and systemic approach to collecting data of attacks on health care. This system utilises the same methodology across countries to address the knowledge gap of the extent and nature of attacks on health care.

Use of Surveillance for administration purposes -

Administrative data are available from a variety of state, federal, and private sources and can, in many cases, be combined. As a tool for planning and surveillance, administrative data show great promise: They contain consistent elements, are available in a timely manner, and provide information about large numbers of individuals. Because they are available in an electronic format, they are relatively inexpensive to obtain and use.

It helps spur 'Good Governance' to citizens in countries, wherein they cannot reach via traditional means to cater to public welfare.

Digitization of document application and updating has helped people from financially weak as well as hard-to-reach background people, in developing and under-developed countries.

Surveillance and its history

Over the course of time, computer vision research has matured significantly. Although some of the core problems, such as object recognition and shape estimation are far from solved, many applications have made considerable progress. Video Surveillance is a thriving example of such an application. On the one hand, worldwide the number of cameras is expected to continue to grow exponentially and security budgets for governments, corporations and the private sector are increasing accordingly. On the other hand, technological advances in target detection, tracking, classification, and behaviour analysis improve accuracy and reliability. Simple video surveillance systems that connect cameras via wireless video servers to Home PCs offer simple motion detection capabilities and are on sale at hardware and consumer electronics stores for affordable rates. The impact of these advances in video surveillance is pervasive. Progress is reported in technical and security publications, abilities are hyped and exaggerated by industry and media, benefits are and dangers dramatised in movies and politics. This exposure, in turn, enables the expansion of the vocabulary of video surveillance systems paving the way for more general automated video analysis.

The history of traditional surveillance dates back to the invention of moving pictures by 'Eadweard Muybridge' created an early prototype called the zoopraxiscope in 1878. Inventors Thomas Edison and William Dickson began experimenting with the idea in the 1880s, but it wasn’t until 1893 that they made the first public demonstration. It instantly captivated the world. Within just a few years, the motion picture industry was up and running. Smaller, portable, hand-held video cameras started to appear by 1939. They were used for surveillance and reconnaissance during World War II. These cameras—both large and small—recorded video footage onto film to be processed and watched later.

Fifteen years after Léon Theremin (Russian Physicist) possibly built a system in the Soviet Union, an engineer named Walter Bruch designed what many consider the world’s first surveillance closed-circuit television (CCTV) system. He built it so Nazi scientists and military personnel could safely observe the launch of V-2 rockets at the Peenemunde Airfield. The American military would later use a similar design to test atomic bombs.

The earliest CCTV security cameras available to the public appeared in 1949. Produced by American company Vericon, they still couldn’t record and required constant monitoring.

Security details extensively used CCTV security cameras during Queen Elizabeth II’s coronation in 1953. In 1960, during a visit by the Thai Royal Family, CCTV again. London Transport installed a few CCTV cameras in the train station in 1961. New York had a few covering Times Square in the mid-60s.

The city of Olean, New York, became the first location in the United States to install security cameras along its main street in 1968. The cameras broadcast video directly to the local police station. Other towns and cities would soon follow suit.

But these systems still required either 24/7 monitoring or a technician to watch the VTR, if you could afford one and change the reels as necessary.

The arrival of consumer videocassette recorders (VCRs) in 1971 pushed adoption even further. This advancement allowed surveillance and security cameras to go mainstream.

Retail shops and banks began installing CCTV systems with integrated VCRs extensively in the mid-70s and into the 80s. These were big, bulky, and conspicuous. With the development of charge-coupled device (CCD) technology in 1976, surveillance cameras could capture footage in low-light situations. This was a major milestone on the path to the true night vision capabilities that cameras have today.

An American company, Kodak, introduced several digital products in 1987. Digital video compression arrived in 1993 with the release of the Ampex DCT. Apple (another American company) brought in digital image capture to consumers with their QuickTake 100 in 1994.

Digital cameras recorded video footage on hard drives and flash storage rather than magnetic tape. The footage is of better quality and does not deteriorate over time like a videocassette. Digital surveillance and security cameras can record days, weeks, or even months of footage before running out of space. That's not including the virtually unlimited storage available in the cloud. And hard drives can be easily erased and reused indefinitely.

The development of digital multiplexers in the mid-90s allowed a single digital video recorder (DVR) to capture and save footage from more than one camera. This led to the multi-camera security systems used now.

Cameras got smaller and more specific, too. This digital migration saw the first IP (internet protocol) camera—the Axis NetEye 200—land in 1996. This removed the need for a closed-circuit system. The camera could transmit footage wirelessly over a computer network. The NetEye is the forefather of modern web and surveillance cameras.

In today's times, Security cameras, dash cams, traffic cameras, and body cams are a part of everyday life practically everywhere. This technology is used by Governments (majorly), Private companies and Individuals alike.

Remarks on the development of surveillance technologies

Time and again, it has been pointed out by various international organizations, independent think-tanks, experts and even government officials regarding the issue of surveillance.

David Kaye, who's the United Nations Special Rapporteur on freedom of opinion and expression, made the appeal as he prepared to present his latest report to the Human Rights Council in Geneva.

He highlighted that while States were largely responsible, companies appeared to be "operating without constraint" too, in a "free for all" private surveillance industry environment.

“Surveillance tools can interfere with human rights, from the right to privacy and freedom of expression to rights of association and assembly, religious belief, non-discrimination, and public participation,” the Special Rapporteur said in statement. “And yet they are not subject to any effective global or national control.”

According to Mr. Kaye’s report, the surveillance of journalists, activists, opposition figures, critics and UN investigators can lead to arbitrary detention.

It has also been linked to torture and possibly to extrajudicial killings, the Special Rapporteur said, citing various ways that States and other actors monitor individuals who exercise their right to freedom of expression.

These include hacking computers, networks and mobile phones, using facial recognition surveillance and other sophisticated surveillance tools to shadow journalists, politicians, UN investigators and human rights advocates.

Firstly, public opinion and acceptance is a shaping factor (among others – technological capability, cost etc.) in the development and deployment of surveillance technologies and surveillance infrastructures. Certain systems and technologies are accepted as necessary or unproblematic, while others are greeted with suspicion and even provoke outrage.

Understanding what drives public perception and opinion on surveillance technologies is, hence, important in the broader comprehension of surveillance systems generally.

Secondly, in a democratic society, public opinion should play a significant role in shaping policy, particularly policy which may impact social structures, or the principles according to which the society is organised. The policies around the deployment of surveillance technologies and the information networks into which they are linked, are examples of such policies (See Solove 2004). Lack of comprehension of the nuances of public opinion, indicates a hole in democratic process in this area.

Contentions of its use

Products or services with intended and unintended surveillance capabilities have the potential to provide positive contributions to a country’s economic, defense, and societal well-being. For example, such products or services can be used to safe-guard election systems from interference.

But too often, surveillance technologies and products are misused by foreign governments to stifle dissent, harass human rights defenders, intimidate minority communities, discourage whistleblowers, chill free expression, target political opponents, journalists, and lawyers, or interfere arbitrarily or unlawfully with privacy.

- Used against journalists
- Used against political oppositions
- Used against activists
- Used for preventive actions
- Used against active citizens

Conclusion

Surveillance is a development that was the product of time, but with the current situation of instability, tensions and repressive regimes, it has become a tool of misuse but to make it effective, ethical and for the welfare of the people is crucial and that makes the discussion to go further in the future, but with a hope of substantive consensus based solutions being proposed by Stakeholders, which are the countries, companies, third parties and lastly, the people, themselves.

Further research links -

- https://news.un.org/en/story/2019/06/1041231
- https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report
- https://privacyinternational.org/learn/mass-surveillance
- https://www.ohchr.org/en/privacy-in-the-digital-age
- https://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET%281999%29168184_EN.pdf
- https://highleveladvisoryboard.org/third-statement-of-the-co-chairs-of-hlab/