Forum: HRC2

Issue: The issue of cyber surveillance targeting civilians

Student Officer: Zeki Mehmet Naamani

Position: Deputy President

Introduction

In the digital era, States and private actors deploy increasingly sophisticated tools-from targeted spyware and device exploits to mass interception, biometric identification, and data profiling monitor people's communications and behaviour. At the same time, some surveillance may be lawful and legitimate when strictly necessary and proportionate, a troubling global pattern has emerged of cyber surveillance targeting civilians, including journalists, human rights defenders, political opponents, lawyers, and ordinary users. Such practices—often secret, inadequately regulated, and lacking oversight—threaten rights to privacy, expression, association, and non-discrimination. This report outlines methods and trends, surveys legal and normative frameworks, highlights abuses and recent developments, and proposes viable solutions for HRC2 delegates.[1]

Definition of Key Terms

Cyber Surveillance

The use of digital technologies (software, hardware, and network-based capabilities) to collect, access, analyse, or interfere with individuals' communications, devices, data, or online activity. It includes both targeted and mass techniques.[1][2]

Targeted Surveillance

Intrusive monitoring directed at specific persons or groups based on an articulated rationale. In human rights law, even targeted measures must be lawful, necessary, and proportionate, with effective safeguards and oversight.

Mass Surveillance

Bulk or indiscriminate collection and processing of communications content or metadata relating to a broad population without prior, objective, and individualised suspicion. International human rights experts have repeatedly questioned its compatibility with privacy and other rights.

Mercenary Spyware

Commercially developed intrusion tools (e.g., Pegasus, Predator, Graphite) were sold to State clients to covertly compromise devices and extract data. Often delivered via zero-click exploits requiring no user interaction.[5]

Metadata

Information about communications (such as time, duration, recipients, location, identifiers) when aggregated reveals intimate patterns and associations, even without content.

Biometric Surveillance

Identification or tracking based on physiological or behavioural traits (e.g., facial images, gait, voice). Real-time remote biometric identification in public spaces has raised serious concerns regarding necessity, proportionality, and chilling effects.

Necessary and Proportionate Principles

A widely used civil-society benchmark distilling how international human rights law applies to communications surveillance: legality, legitimate aim, necessity, proportionality, due process, transparency, public oversight, and effective remedy.[2]

Background Information

Recent developments in 2024−2025 underscore the escalating threat of mercenary spyware alongside nascent efforts toward global norm-setting in technology. This period saw widespread alerts, beginning in April 2024 when Apple issued threat notifications in over ninety countries, warning journalists, dissidents, and human-rights defenders of suspected mercenary-spyware attacks, with subsequent rounds extending this to nearly one hundred nations. These warnings were followed by concrete forensic confirmations in 2025, where independent researchers reported fresh intrusions against European journalists and activists using Paragon's Graphite spyware, illustrating the continuing and global spread of commercial surveillance tools. In parallel, global bodies moved to establish safeguards: the UN General Assembly adopted the United Nations Convention against Cybercrime in December 2024, prompting international debate, while the EU's AI Act (2024−2025) advanced with restrictions on harmful AI uses, specifically banning untargeted scraping for facial recognition databases and certain biometric categorization practices.

Major Countries and Organisations Involved

Office of the United Nations High Commissioner for Human Rights (OHCHR)

Issues thematic reports on privacy in the digital age (A/HRC/48/31; A/HRC/51/17), emphasising legality, necessity, proportionality, transparency, oversight, and effective remedy; calls out abuse of intrusive hacking tools and highlights the protective role of encryption.[2]

UN Special Rapporteur on the right to privacy

Engages States on privacy-related practices, conducts country visits and reports to the HRC and General Assembly, urging stronger safeguards and access to remedy.[2]

Member States and regional bodies

Diverse approaches: some have robust oversight and transparency; others rely on secretive frameworks. The European Union has adopted the AI Act with restrictions on biometric systems and data practices; the United States has taken export-control and sanctions measures concerning certain spyware vendors.[3]

Technology companies

Platform providers and device manufacturers (e.g., Apple) provide threat notifications, hardening (e.g., Lockdown Mode), and vulnerability patching. At the same time, a commercial surveillance industry develops and markets intrusion tools to government clients.[5]

Civil Society and Research Labs

Groups such as Amnesty International's Security Lab, Access Now, and The Citizen Lab conduct forensic investigations, support victims, and advocate for moratoria.[11]

Viable Solutions

Several viable solutions are proposed to address issues related to surveillance and digital rights. These solutions begin with the need to align domestic surveillance law and practice with international standards. This involves adopting legislation that strictly limits surveillance to what is lawful, necessary, and proportionate for a legitimate aim, requiring prior independent authorization (preferably judicial), clear time limits, data minimization, and deletion duties, while also protecting encryption and narrowing any exceptional access. Furthermore, this alignment requires establishing independent oversight bodies with access to classified information and the mandate to audit, publish aggregate statistics, and receive complaints. A second crucial solution is to regulate the commercial spyware market by introducing licensing, export controls, and procurement rules anchored in the UN Guiding Principles on Business and Human Rights. This regulation should also mandate human-rights due diligence, transparency on end-users, complaint mechanisms, and meaningful penalties and sanctions for abuses, including listing and targeted financial measures against firms or operators that facilitate violations. [1]

The third solution focuses on safeguarding civic space and the work of journalists by mandating enhanced protections for human-rights defenders, journalists, lawyers, and opposition figures, who are frequently targeted. This includes funding emergency digital-security support, legal aid, and forensic assistance, as well as requiring prompt user notification by providers when technically feasible and compatible with investigations, and ensuring access to effective remedies and reparations. Additionally, to protect public freedoms, the fourth solution advocates for reining in biometric surveillance in public spaces

by prohibiting untargeted scraping and blanket real-time remote biometric identification in publicly accessible spaces. If any uses are permitted, they must be confined to narrowly defined exceptional circumstances with prior judicial authorization, strict necessity tests, logging, independent audits, and sunset clauses. Addressing the international dimension, the fifth solution calls to promote international cooperation with safeguards. This entails negotiating and interpreting cross-border cooperation (including under the new UN cybercrime treaty) to embed human-rights safeguards, dual criminality, oversight, and redress, encouraging mutual legal assistance that respects privacy and due process, and considering the establishment of a specialized UN mechanism or registry for cross-border surveillance notifications and remedies. [12]

Finally, to ensure the long-term effectiveness of these measures, the sixth solution is to build technical resilience and capacity. This involves supporting secure-by-default device settings, vulnerability disclosure and patching ecosystems, promoting end-to-end encryption, expanding resources such as lockdown modes for high-risk users, and funding independent labs that can detect and attribute intrusions. It also includes providing capacity building to regulators, judges, and national human-rights institutions. [7]

Bibliography

1. Office of the United Nations High Commissioner for Human Rights (OHCHR). “The right to privacy in the digital age.” A/HRC/48/31, 15 Sept. 2021. .
2. OHCHR. “The right to privacy in the digital age.” A/HRC/51/17, 4 Aug. 2022. .
3. United Nations General Assembly. “United Nations Convention against Cybercrime.” A/RES/79/243, 24 Dec. 2024. . [6]
4. European Parliament. “Artificial Intelligence Act: MEPs adopt landmark law.” 13 Mar. 2024. .
5. European Parliament Topics Page. “EU AI Act: first regulation on artificial intelligence.” 19 Feb. 2025. .
6. U.S. Department of the Treasury. “Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium.” 5 Mar. 2024. .
7. Apple. “About Apple threat notifications and protecting against mercenary spyware.” 23 Apr. 2025. .
8. TechCrunch. “Apple alerts users in 92 nations to mercenary spyware attacks.” 10 Apr. 2024. . [4]
9. Amnesty International. “Apple threat notifications: What they mean and what you can do.” 11 Apr. 2024. .
10. The Citizen Lab. “By Whose Authority? Pegasus targeting of Russian- and Belarusian-speaking opposition and media in Europe.” 30 May 2024. .
11. The Citizen Lab. “First Forensic Confirmation of Paragon's iOS Mercenary Spyware ‘Graphite’ Finds Journalists Targeted.” 12 June 2025. .
12. Columbia Global Freedom of Expression. “Resolution 54/21 – Right to privacy in the digital age.” 2023.
13. OHCHR. “Guiding Principles on Business and Human Rights.” 2011. .