The growth of digital technology has transformed practically every component of human life, from communication and education to political engagement, healthcare access, and economic mobility. However, this digital revolution has also brought forth fundamental vulnerabilities that expose people and communities to systemic instability, misinformation, surveillance, and cyberthreats. Because of this, cyberspace security, the safeguarding of digital infrastructure, data integrity, and personal data has emerged as a critical human rights concern. A person's safety, dignity, autonomy, and capacity to exercise fundamental rights in the digital era are increasingly dependent on the security of the systems that surround them. This essay argues that the right to cyberspace security is a fundamental human rights issue, closely tied to equality, privacy, freedom of speech, and political engagement, rather than merely a technical issue.

Stephen P. Marks (2016) points out that human rights are anchored on defending human dignity and enabling individuals to live free from fear and hunger. In the digital era, anxiety increasingly comes from cyber harms: identity theft, data breaches, online misconduct, state surveillance, and algorithmic exploitation. People are vulnerable to privacy violations, prejudice, and manipulation when digital systems lack security measures. Cybersecurity is a logical extension of the right to personal security, as Marks points out, because human rights frameworks evolve in response to new social threats.

The Right to Privacy in the Digital Age (2022) by the OHCHR makes a clear connection between cybersecurity flaws and violations of human rights. It argues that inadequate digital safeguards allow governments and business organizations to violate rights, including equality, privacy, freedom of speech, and due process. Therefore, cybersecurity serves as a preventative and protective mechanism; without it, other rights are vulnerable.

Shashi Tharoor's speech on universality emphasizes how, although human rights must be applied to every person equally, their application differs around the world. This disparity shows itself in cyberspace as unequal access to safe technology. Advanced cybersecurity

infrastructures help wealthier countries and communities, whereas vulnerable populations, such as refugees, low-income individuals, the elderly, and residents living under authoritarian regimes are more vulnerable. This uneven vulnerability produces a two-tier digital environment that threatens universal human rights.

For example, digital technologies are essential to the safety, communication, and documentation of migrants and refugees. The documentary Human Flow by Ai Weiwei subtly illustrates how critical communications and geolocation data might be exposed via digital instability, endangering displaced communities. Similarly, elderly persons who rely increasingly on digital banking, telemedicine, and online communication suffer new types of exploitation without proper cybersecurity understanding, highlighting the limits of digital universality. Cyber insecurity also disproportionately impacts women, the elderly, and underprivileged populations. Online harassment impedes women's ability to participate in public life, according to UN Women (2022). In the meanwhile, older individuals suffer the greatest financial losses from cyber scams globally, according to the AARP and FBI Internet Crime Complaint Center. This indicates a direct danger to their rights to property, safety, and freedom from exploitation. These effects highlight how cybersecurity breaches become weapons of injustice and prejudice. Even while young people frequently dominate digital culture, older folks are depending more and more on digital technology for basic functions including online banking, government services, healthcare portals, and family communication. Yet this group suffers structural disadvantages: lesser digital literacy, limited formal training, and a higher risk of trusting bogus claims. The 2023 FBI IC3 Elder Fraud Report states that cyber-enabled frauds, including phishing, romance scams, and tech-support fraud, cost individuals over 60 over $3.4 billion worldwide. The rights to property, personal security, and a dignified life free from coercion are all violated by these attacks.

Because they are thought to be less tech-savvy, more trustworthy, and financially secure, scammers frequently target elderly folks. The lack of state-backed cybersecurity

education for elders implies a failing to safeguard vulnerable people, showing a gap between digital innovation and human rights commitments. NGOs including the Global Cyber Alliance, HelpAge International, and AARP have demanded that older digital protection be explicitly acknowledged as a human rights concern. Several international laws indirectly support cybersecurity as a human right such as The Universal Declaration of Human Rights (UDHR): guarantees security of person, privacy, and freedom from exploitation, The International Covenant on Civil and Political Rights (ICCPR): protects privacy, expression, and freedoms vulnerable to digital intrusion, and The Madrid International Plan of Action on Ageing (2002): recognizes the need to protect older persons from abuse, including financial exploitation, an increasingly digital phenomenon. However, none of these regimes specifically address cybersecurity for the elderly as a protected rights category.

Strong cybersecurity is necessary to protect privacy and dignity, according to the OHCHR's digital rights reports from 2022 and 2023. They do, however, recognize that vulnerable populations, especially older persons, who suffer disproportionately from cybercrime and digital exploitation are also not adequately protected by the state. The gap continues to grow because there is no global standard for protecting elderly users. This absence puts millions of elderly individuals exposed to preventable damage, compromising global commitments to human dignity, equality, and nondiscrimination.

Accessible and safe technology are essential for ethical cyber protection for the elderly. While excessively basic security solutions expose older folks to frauds, overly complicated ones may unintentionally restrict them autonomy in digital settings. This tension points out the necessity for universal design principles. The lack of comprehensive cybersecurity measures, rather than a lack of technology, puts the rights of elderly people at risk. This is a type of digital discrimination. This imbalance defies Tharoor’s argument for universal rights and shows a key ethical obligation for governments and companies.

Now lets start with what has to change. Our government should establish global human rights standards for cybersecurity. A legally enforceable international agreement should mandate accessible features in digital platforms, promote secure-by-design technology, regulate age-targeted frauds, and provide clear protections for senior citizens. Along with that countries should strengthen national laws protecting digital rights. Countries have to implement solid consumer protection legislation, criminalize cross-border elderly cyber fraud, and enforce clear reporting methods for senior victims of digital crime.

Another thing we could do is expand equal access to cybersecurity education. Governments and non-governmental organizations should create specialized cybersecurity training for senior citizens, such as community seminars, digital literacy initiatives, and streamlined instructions on spotting scams. Lastly, thre should be an increase in transparency and accountability. Businesses need to make a commitment to algorithmic accountability, transparent data practices, and scam-resistant design, especially when it comes to deceptive or manipulative material that disproportionately targets elderly citizens.

Cybersecurity is interwoven from modern human rights. Without safe digital systems, the rights to privacy, dignity, autonomy, property, and freedom from exploitation become fragile. As Marks reminds us, human rights frameworks develop with social requirements; now, cybersecurity sits at the forefront of that transformation. Ensuring digital security for all; including the elderly, is not only a technological aim but a moral and political need for safety, equality, and human dignity.

Citations

AARP. (2023). *AARP Fraud Watch Network: Insights and analysis on scams targeting older adults*. AARP. https://www.aarp.org

DeNardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No Off Switch.* Yale University Press.

FBI Internet Crime Complaint Center. (2023). *Elder Fraud Report 2023.* U.S. Department of Justice. https://www.ic3.gov

International Committee of the Red Cross. (2021). *International humanitarian law and cyber operations: Position paper.* ICRC. https://www.icrc.org

Marks, S. P. (2016). *Human Rights: A Brief Introduction.* Harvard FXB Center

Office of the United Nations High Commissioner for Human Rights. (2022). *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights.* United Nations.

Office of the United Nations High Commissioner for Human Rights. (2023). *Human rights and the digital environment.* United Nations.

Tharoor, S. (2000). *Are human rights universal?* World Policy Journal, 13(4), 1–7.

UN Women. (2022). *Online violence against women and girls: A global review.* UN Women. https://www.unwomen.org

Zuboff, S. (2019). *The Age of Surveillance Capitalism.* PublicAffairs.