Cyberbullying and Cyber Human Rights: The Case of Iran

Mehrak Rahimi

With the quick expansion of the information and communications technology (ICT) infrastructure, almost all people of all walks of life across the globe are given access to the virtual world and its vast possibilities. People in different regions and countries are now connected with the click of a mouse or just a touch of the screen of a smartphone. One of the key reasons of people in using the Internet is to connect to each other and communicate via social media to make communities of shared interest and opinion. The advantages of the virtual world and the Internet are endless and the educational, commercial, industrial, and even entertainment benefits are countless. As a consequence, many governments expand the technological infrastructures and use of new technologies to facilitate increase convenience in life. This situation changed the personal and professional lives of people and the way they perceive the world around them.

Based on the theory of technological determinism, technology is now related to almost all activities of human beings and is so much correlated to power, wealth and knowledge. Any society that targets a prosperous future needs to keep up with the pace of technological development, expand its information technology (IT) infrastructures according to global or regional standards and raise the IT literacy and competencies of their people. The penetration of technology into the society and how technologies are being used for educational, industrial, social, and economic advancement now constitute an index of a country's development and prosperity.

With all that being said, the negative side of using ICT raised many controversies about the way access to technology should be granted to different people:

> All over the world, numerous concerns and issues have been raised, ranging from online safety and security (identity theft, scams, system phishing, hacking, online predators and cyber bullying) to misuse of information (plagiarism, access to inappropriate contents, and misrepresentation) to health and mental hazard (long exposure to screen, back and arm pains, and game/internet addiction) (Tan, Park, Patravanich, & Cheong, 2014, 1-2).

On one hand, many now are discussing if limiting access to technology affordances is a violation of human rights. On the other hand, many believe that technology use without limitation and required legislations leads to the rise of modern crimes that ultimately goes against the benefits of modern technology to the society and human rights.

"The Asia-Pacific (AP) region has not been exempted from various forms of ICT abuses, including spamming, intellectual property infringement (plagiarism and piracy), addiction, delinquency, health and wellness issues, cyberbullying, identity theft, fraud/ scams, pornography, and online sex trafficking" (Tan, Park, Patravanich, & Cheong, 2014, 1-2). Iran, as a developing country in this region, is now experiencing such a situation. With a high rate of educated young population, people demand free access to any type of technology for entertainment and social relationships. Technology and its affordances are used in Iran basically to make virtual communities; thus social media is so popular in the country.

There are now forty-eight million smartphones in use in Iran, with forty seven million social media users (techrasa.com). More than half of the Internet users in Iran are young people and adolescents. Although the purchase of mobile phone lines is restricted for minors in Iran, many parents provide their minor children with mobile phones and Internet access and many of these young people are active members of social media.

Although certain benefits for social networking have been reported for young people such as "self-presentation, learning, widening their circle of relationships, and managing privacy and intimacy" (Livingstone & Brake, 2010, Bhat, Chang, & Linscott, 2010, 35), risks of using such environment without supervision such as the "loss of privacy, bullying, and harmful contacts" (ibid.) are also noted. The penetration rate of Internet (45.3 percent), computer use (41.2 percent) and mobile use (77.9 percent) in Iran shows that many Iranians now are using mobile social networking. This indicates a kind of omnipresent use of social media in Iran, signaling certain social and individual advantages and disadvantages.

The ubiquity of technologies and the use personalized technology tools particularly combined with technology literacy, awareness, and caution can lead to enhancement of education. The benefits of mobile learning has been documented and many developed countries are now directing the potentials of the Internet and mobile social networking on collaborated learning via

mobile learning (m-learning). The use of m-learning has opened doors to lifelong learning and education for everyone, anytime, anywhere.

However, when technologies are introduced to the country without cultural agendas and/or careful execution of strategic plans, the villainous potentials of the Internet show up and criminals take over the control of communication, interactions, and relationships. One such danger of social networking includes cybercrime. Cybercrime is defined in Iran as

> cases of intrusion into computers or information network systems (computer systems) without justifiable access privileges or access which exceeds permitted access privileges or causing damage, destruction, or alterations to systems, data, programs and causing disruptions (impairing performance or causing system failures) in communication networks (computer systems) (cyber.polic.ir).

Cybercrimes frequently take place in three main domains in the Iranian context: economic, social, and ethical. It is reported that more than 80 percent of cybercrimes are related to account theft and data leak. These types of crime cause both emotional and physical damage to the victims and can ruin their personal and emotional lives. For a country like Iran where cultural values play a huge role in relationships, the spread of personal and private data may do a lot of harm to users, especially young people and female members of the social networks.

The government has tried to control cybercrimes by enacting new legislations and implementing filtering policy. However, the slow pace in adopting strategies to prevent cybercrimes and educating users of the cyberspace is observed. This has now created complicated situations in the country, increasing the number of victims, and spreading pessimistic views on the value of IT tools. The rate of fraud, defamation, and cyberbullying in the country shows that people are not aware of the dangers of the cyberspace and are required to be educated with respect to cyber dangers and rules/regulations to be able to defend their cyber human rights.

Cyberbullying

While meeting in person needs identity revelation, in a virtual world people can have hidden, unknown, and fake identities. This actually opens up many

opportunities for intruders and cyber criminals. Actually, many criminals have found safe places in the cyberspace and are now more courageous to do any type of crime where their true identity seems to be difficult to be revealed. Many of these criminals have extended their illegal activities into the cyberspace or have invented new ways for fraud and felony.

As new types of crimes, or cybercrimes, developed and emerged with the advent of new technologies, new prevention strategies and legislations are required for the societies of the 21st century. People's awareness of the dangers they or their family members may face, cautions they must exercise while sharing their personal information with others, and how the law could protect them against any cybercrime and protect their human rights in cyberspace are just a few things people should know before or while they get involved with the Internet or any type of social media.

Cybercrime is also defined as "the use of information and communications technology to intimidate, harass, victimize, or bully an individual or a group of individuals" (Bhat, Chang, & Linscott, 2008, 54). In other words, cybercrime is a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes) (www.techopedia.com). Different types of cybercrimes have been identified such as identity theft, spam and phishing, malvertising (malicious advertising), and stalking or cyberbullying. Yet, whether cyberbullying is a serious case of cybercrime or not is open to contradiction. Cyberbullying in its mild status can be just like any face-to-face offense. Many of us do not take action against offenders, unless the situation goes seriously wrong.

To bully in general means "to threaten to hurt someone or frighten them, especially someone smaller or weaker."[1] In the same vein, cyberbullying is a type of bullying that takes place in cyberspace or by using digital devices like cell phones, computers, and tablets. As a result, cyberbullying can happen both offline and online, while in both cases technological devices are involved. People can be bullied by Short Message Service (involving only text) and Multimedia Message Service (involving photos and videos). The situation worsens when people are bullied while using the Internet especially social media (such as Facebook, Instagram, Telegram, etc.) where people voluntarily share private information of various types including personal photos, bank account numbers, social security numbers, addresses, and many other information. Someone who cyberbullies may access some-

one's private information without permission and/or with a cunning plan and then send, post, or share negative, harmful, false, or mean content about the person (www.stopbullying.gov) and ruin the person's social and professional integrity. The cyberbully may even go on with blackmailing or forcing people to do things against their will. Examples of cyberbullying include:[2]

- Posting hurtful messages, images or videos online;
- Repeatedly sending unwanted messages online;
- Sending abusive texts and emails;
- Excluding or intimidating others online;
- Creating fake social networking profiles or websites that are hurtful;
- Nasty online gossip and chat; and
- Any other form of digital communication which is discriminatory, intimidating, intended to cause hurt or make someone fear for her/his safety.

There seems to be some major differences between traditional bullying and cyberbullying. Traditional bullying is mainly physical and is traceable in the immediate environment. It may have negative effects on a person that may heal or be forgotten after the passage of time when the person is not present in that specific location and has freed her/himself of the bad memories of the events. However, cyberspace provides a permanent damage and the wound does not heal as the information spreads among other communities and even globally. This creates some sort of power differential between the cyberbully and the target, as the cyberbully has certain types of information (videos, personal messages, photos, document) that give them power to "hurt, shame, victimize, or harass the target" (Bhat, Chang, & Linscott, 2010, 37). Another important point is that "cyberbullying often has a component of sexual harassment (ibid.) and that may lead the target to "keeping silent out of embarrassment" (ibid.). In traditional societies, this damage to young girls' life cannot be healed very easily and some serious consequences (such as revenge, suicide, etc.) may occur.

Some empirical studies on cyberbullying show that cyberbullying is a universal problem and any society with connection to the Internet may experience it. A Microsoft study done in 2012 among twenty-five countries of the Asia Pacific region shows that China, Singapore, and India had the highest rates of online bullying (70 percent, 58 percent, 53 percent of surveyed children aged 8 to 17 years respectively) (Tan, Park, Patravanich, & Cheong,

2014, 2). Jaghoory, Björkqvist and Österman (2015) compared differences in frequencies of both victimization and perpetration of cyberbullying among adolescents from Iran and Finland. Their results showed that both victimization and perpetration of cyberbullying of all kinds were clearly more frequent in Iran.

Certain studies have also paid attention to the reasons why people are easily targeted and hunted by cyberbullies. Brighi et al. (2012) reported that traditional bullying has a correlation with cyberbullying and being either a direct or an indirect victim of traditional bullying was a very strong predictor for becoming also a victim of cyberbullying for both males and females.

Sourander et al. (2010) suggested that cyber victimization was related to psychiatric and psychosomatic problems such as family issues while cyberbullying was related to perceived difficulties, hyperactivity, conduct problems, frequent smoking, and drunkenness.

Depression (Yabbar, 2004), loneliness (Sahin, 2012), self-esteem (Brighi et al, 2012), bad relationship with parents, and gender (Olenikin-Shemesh et al., 2012) can be indications of being victims of cyberbullying or being cyberbullies.

Information Technology Policy of Iran

Iran is located in central Asia with a surface area of 1,628,750 square kilometers and a population of more than eighty million people. Based on United Nations data, the country's mobile-cellular subscriptions (per one hundred inhabitants) in 2014 was 93.4 percent and individual rate of Internet use was 44.1 percent. [3]

Based on Iran's 1404 Perspective Document (20 Year National Vision), Iran should be ranked first in the region by 2026 with respect to economy, science and technology.[4] As a result, the scientific and technological infrastructures of the country are being developed based on the agendas defined by the national development policies.

The strategic plan on IT of the country was adopted in 2007 to enable the country to reach the defined goals with respect to ICT use in five domains of technology, economy, society, politics, and culture. The strategic plan is supposed to be the main guideline that clarifies the role of the state-of-the-art technologies in the different aspects of Iranian lives at the personal and professional levels.

The value of this document considering the Constitution, the 1404 Perspective Document and the general IT policies of Iran is seen in several aspects:

- Protection of human integrity, legitimate freedom, and individual and social ethics;
- Spread of social justice and free sharing of information;
- Guarantee of social, political, and economic security of the country;
- Enhancement of Islamic-Iranian identity and the expansion of use of the Persian language in the cyberspace;
- Realization of a knowledge-based society, reliance on social capital; and
- Enhancement and fortification of religious democracy.

Therefore, the mission statement of ICT policy in Iran is

> Providing suitable access for people in all walks of life to IT and inclusive education of the society, educating professional human resources for applying IT in all aspects of life, and creating competitive atmosphere for organizing networked and smart society that leads to a change of pattern and process of national development from basic resources to basic knowledge; and educating responsible citizens in acquiring the values and filling the national digital gap with the global society (page 18).

The strategies of the country to expand the IT infrastructures in order to improve the people's sense of identity as Iranians are based on the following considerations:

1. Expansion of the use of the Persian language and promotion of Iranian-Islamic culture in the cyberspace (e.g., designing appropriate e-content);
2. Providing safe and equal IT opportunity for every citizen (e.g., protecting human rights in cyberspace);
3. Promoting social awareness and IT literacy; and
4. Ensuring a secure society for Iranian families while using the cyber services.

Sequentially, the country invested hugely on the expansion of the ICT infrastructure in the last decade. Based on a recent report by the International

Telecommunication Union (ITU) in 2016, Iran's ICT Development Index (IDI) is 4.99, 0.92 points above the average for developing countries. Iran is ranked 85 in 2016 and 81 in 2017 among 176 countries in IDI.[5] Iran was ranked 14th in IDI in the region of the Middle East. Considering the rank improvement, Iran was ranked second in the region, behind Jordan (techrasa.com).

Cyberbullying in Iran

Based on ITU's 2016 report, around 45 percent of Iranians used the Internet in 2016. However, Internet is mainly used for entertainment purposes in the country. Iranians show particular interest in using social media especially Instagram, Facebook, and Telegram. It is reported that the main online activities of Iranians include using social media, playing game and watching movies. However, online distance work, blogging, online classes and online consulting are not favorite uses of the Internet among Iranians (techrasa.com). What the report suggests is that the nation is just aware of one function of the cyberspace that is interaction and communication. Some academics believe that this type of communication is not suitable to the Iranian society as it creates problems for Iranian families when they ignore ancient customs such as visiting their elders and siblings. It has even been suggested that the use of cyberspace is related to low rate of marriage and birth in Iran in the recent decade.

In spite of the reports of bad effects of overuse of the Internet, the use of social media is very popular among Iranians. Telegram, in particular, has attracted the attention of Iranians and has become the most popular messaging app in Iran because of its groups, channels, games, and stores. Telegram has more than forty million users in Iran and is said to consume 40 percent of Iran's internet bandwidth. With this profound impact, different types of cybercrimes are inevitable in such an environment. According to an official report by Iran's Cyber Police, 66 percent of cybercrimes in Iran take place on Telegram, 20 percent on Instagram and less than 2 percent on WhatsApp. While authorities have repeatedly warned the nation to take wise and cautious actions while using the cyberspace, many Iranians are still unaware of the possible danger posed by cybercriminals. This actually explains why the rate of cybercrimes is slightly escalating in the country.

Cyber safety, rights, and wellness have become vital issues among the governments in the Asia-Pacific. The responses to these issues vary from strict regulations on ICT use (i.e., access restrictions like censorship and filters) and self-regulation programs (i.e., awareness campaigns and education programs) (Tan, Park, Patravanich, & Cheong, 2014, 12). Iran is not an exception in this regard. The country now is using intelligent filtering to filter inappropriate e-content such as general pornography, child pornography and gambling. The government also highly recommends the use of local social networking such as Soroosh instead of Telegram to safeguard the users' private information and prevent cyberbullying.

In spite of such prevention plans, cybercrimes are taking place in the country on a daily basis. Iranians do not embrace the local social networks, use VPN (Virtual Private Network) on desktops and cellphones to access the blocked content, and seem to be indifferent to warnings given by the authorities to safeguard their personal information. One of the most common cyberbullying cases in Iran is the hijacking of personal information and blackmailing the victims on the spread of their personal information to the public. Young girls and married women are among the top of the list of victims of cybercrimes in Iran. The cyberbully may ask for money to destroy or return the data, unethical behavior, or cooperation in illegal acts such as robbery or assistance in other cybercrimes. Defamation of users and spreading rumors both about famous (celebrities) and ordinary people are also common in the cyberspace. The key to preventing cyberbullying is in educating and making people become aware of the consequences of such unethical behavior. This is the missing chain of the IT policy in Iran.

Cyber Legislations in Iran

The Supreme Council of Cyberspace is the higher authority of the country to decide for the national IT policy. The head of the Supreme Council of Cyberspace is the President of Islamic Republic of Iran. There are higher commissions under the supervision of the Council:

- Higher Commission of Legislations;
- Higher Commission of Promoting E-content;
- Higher Commission of Security.

The Higher Commission of Legislations is responsible for policymaking and monitoring of the cyberspace including issuing rules and regulations related to security, content, accessing and pricing, types of service, infrastructures, cybercrimes, and user's cyber rights. The Higher Commission of Promoting E-content is responsible for supporting the cultural products and expanding e-commerce by both private and public sectors. The Higher Commission of Security is responsible for guaranteeing highly secured internet access for the country and availability of cyberspace specialists and protecting the national infrastructures from national/international cyber-attacks.

Based on existing legislation, authorities have taken different types of action to limit the occurrence of cybercrimes. In addition, in order to lower the destructive impact of cybercrimes, Iran's Cyber Police was established in 2011. The organization's aim is to prevent, investigate and combat cybercrime. The organization explains the aim of its establishment as follows:

> The purpose of establishing cyber police is to secure cyberspace, to protect national and religious identity, community values, legal liberty, national critical infrastructure against electronic attacks, to preserve interests and national authority in cyberspace and to assure people in all legal affairs such as economic, social and cultural activities in order to preserve national power and sovereignty. (cyber.police. ir)

Different types of cybercrimes have been listed by the Cyber Police such as

- Crimes with information network infringement (e.g., hacking, data leaking);
- Crimes involving the use of Information Network (gaming fraud, shopping mall fraud);
- Cyber copyright infringement;
- Crimes involving illegal contents (pornography, gambling);
- Cyber defamation (insult, cyber stalking).

There are strict rules in Iran to safeguard users' rights in the cyberspace in the following domains: e-commerce, cybercrimes, criminal contents, and the places that offer cyber services (Coffee-nets). The punishment for violating personal rights includes imprisonment and fine.

Remaining Issues

Although the Iranian authorities had initiated good measures to promote the use of IT, give suitable IT access to the people, and make the cyberspace secure for all users, there are still steps that should be taken especially with respect to cyber citizenship, identity and human rights.

1. Cyber identity and citizenship

In this era of IT, new identities are getting shaped. People of the 21st century have different perceptions of the world in comparison to their parents. The digital natives perceive the world via technologies and this perception can be essentially different from digital immigrants, their parents, teachers, and the authorities. Therefore, the citizens of this era should now behave responsibly and watch cyber ethics and "netiquette" while they are online. This is especially achieved by making them familiar with their new identities, rights and responsibilities; and making them aware of the possible threats and harms of the virtual world.

In Iran's national policy issuances, this identity is defined based on the agendas of the local culture and the values of Iranian society. Iranian cybercitizens, like any other user, are expected to utilize technology in an appropriate manner, taking care of their online safety, being responsible for their behavior, avoiding harming people, and respecting their own and others' cyber human rights.

2. Awareness programs

One observed weakness of IT policy in Iran is negligence of awareness programs for parents, teachers and young users. Any program on cyber human rights should include making people become aware of these rights and the way they can fight those who violate their rights. People should be aware of the way they can secure cyber use (such as creating strong passwords, attention to their own privacy and that of others, creating and sharing appropriate contents) and the way the government provides them with safe and secure connections.

3. Promoting the educational values of ICT

Iranians are reported to use the Internet mainly for entertainment purposes. More than half of the users are subscribers of just one mobile social

network. The frequency and variety of cybercrimes in this environment are abundant. Therefore, the educational and scientific values of ICT should be highlighted in schools and academic centers for young people.

4. Restricting cyberbullying

Cyberbullying has long emotional effect on people's personality, life and social relationship because of the deletion of the information that has been shared online takes a lot of time. Therefore, strict rules are required to prevent cyberbullying. What is expected from the authorities and policymakers is to take serious actions against cyberbullying to protect the wellness and security of the country. In this regard, young and female users are more vulnerable and thus need more attention.

5. Rehabilitation programs for offenders and victims

Another important aspect of cyber human rights is the way the authorities punish the offenders and help the victims recover from the adverse effects of cyberbullying. The country needs research and development programs to establish rehabilitation centers for cyberbullies and their victims. Why some people bully others online and why some are trapped and caught in the cunning plans should be researched in the Iranian context and treatment policies should be developed.

6. Cyber human rights declaration

The Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966) were adopted to make the lives of people safer and more secure. Now in the digital era, people need an international Cyber Human Rights Declaration to be adopted by international organizations. This international declaration can help people become aware of the way they can freely share information without violating other people's privacy. This can be related to different domains such as:

- Online freedom of speech;
- Avoidance of gender and ethical biases;
- Respecting the rights of users;
- Accessing and sharing data; and
- Protecting one's privacy while sharing information.

Educational Initiatives

Educators should be well-informed of the dangers of cyberbullying. In this regard, while the Ministry of Education plays a key role in approving strict rules and regulations to avoid cyberbullying among students, the importance of its role in educating young users of the probable consequences of their actions is undeniable. Recently, the Ministry of Education has started offering courses for teachers and education officials that cover cybercrimes and how to avoid them. The courses are held both electronically and face-to-face and are required courses for teachers to be able to get tenure.

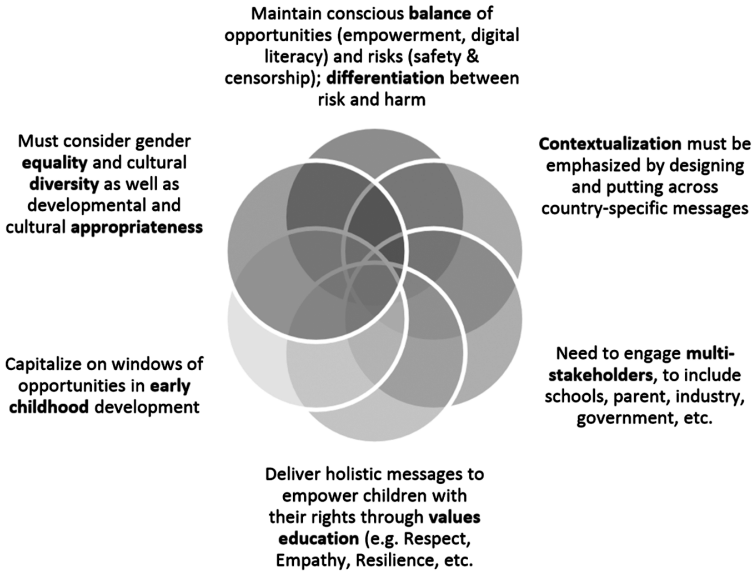
Some schools in Iran hold workshops for students and teach them about the opportunities and threats of the cyberspace. These courses are held especially for girls, as they seem to be among the targets of cyberbullies in Iran.

Meticulous planning on a number of measures regarding cyberbullying by Iranian educators covers the following:

1. Research on
    a. the status of cyberbullying in Iran in order to have a clear picture of the current situation
    b. the psychological, social, and economic reasons of cyberbullying among Iranians;
2. Promotion of cyber human rights and making people become aware of their rights;
3. Promotion of IT literacy of students and their parents to make them familiar with the state-of-the-art technologies; and
4. Education of young students and female users on the dangers of the cyberspace, how to handle the problems arising from it.

A number of key points suggested to be considered in the areas of research, policy, partnerships, and capability-building when developing programs are meant to build digital citizenship through safe and responsible use of ICT (Tan, Park, Patravanich, & Cheong, 2014, 44) as shown in Figure 1. Therefore, these issues should be considered seriously in dealing with the way young people are being prepared to use ICT.

Figure 1. Key points in program design and implementation on safe digital citizenship



Digital citizenship is considered a crucial competency for teachers and students of the 21st century and thus any educational initiative should consider certain standards in their movement as suggested by International Society for Technology in Education (ISTE). These standards include: standards for students, educators, administrators, coaches, and Computer Science (CS) educators. The standards for teachers and students with respect to digital citizenship are summarized in Table 1.[6]

Table 1. ISTE standards for students and educators regarding digital citizenship

1. Standards for students	a. Students cultivate and manage their digital identity and reputation and are aware of the permanence of their actions in the digital world. b. Students engage in positive, safe, legal and ethical behavior when using technology, including social interactions online or when using networked devices. c. Students demonstrate an understanding of and respect for the rights and obligations of using and sharing intellectual property. d. Students manage their personal data to maintain digital privacy and security and are aware of data-collection technology used to track their navigation online.
2. Standards for educators	a. Create experiences for learners to make positive, socially responsible contributions and exhibit empathetic behavior online that build relationships and community. b. Establish a learning culture that promotes curiosity and critical examination of online resources and fosters digital literacy and media fluency. c. Mentor students in safe, legal and ethical practices with digital tools and the protection of intellectual rights and property. d. Model and promote management of personal data and digital identity and protect student data privacy.

Considering what has been mentioned, the components of a cyberbullying prevention course for Iranian students are suggested in the following section.

Cyberbullying Prevention Course for Iranian Students - A Proposal

The educational system of Iran needs to integrate regular courses on ICT use and digital citizenship into the primary and secondary school curriculums to promote cyber safety and cyber human rights. This would also guarantee a better return on the investments made in recent years regarding this important issue by both public and private sectors in Iran. This cyberbullying prevention course proposal is briefly discussed below. The components of the course are designed based on several frameworks including Iran's national policy documents, literature review, cyber citizenship standards, and UNESCO's guidelines on Education for International Understanding.

The proposed program would be implemented in the Iranian context to address the following issues with respect to safe ICT use:

- Cyber identity;
- Cyber health (physical/psychological);
- ICT literacy;
- Cyber delinquency;
- Information security management;
- Communication skills (in cyberspace);
- ICT entrepreneurship;
- Cyber netiquette; and
- Cyber citizenship rights (human rights).

The proposed program fills the gaps that exist in the Iranian educational system with respect to cyber identity, cyber human rights, cyber netiquette, democratic dialogue in cyberspace, and respecting diversity in virtual world.

It is designed and implemented with the hope of changing the attitudes of cyberspace offenders (those who victimize people through cyberbullying) and promote in them the sense of empathy, understanding and acceptance. The cyberspace offenders are also expected to become aware of the consequences of their acts on other students' lives.

It also aims at making students become aware of the ways cyberbullies may trap them and how they can arm themselves with necessary knowledge

(e.g., ICT literacy) to make safe use of cyberspace. Last but not least, the program aims to help the victims of cyberbullying show bravery to fight cyberbullies by guarding against mean people and recovering from the adverse effects of cyberbullying.

The goals of the proposed program are organized in three main categories including cognitive, socio-emotional, and behavioral. The aim of cognitive component is to make students become aware of the facts (e.g., rules), causes, and impacts of cyberbullying and strategies to prevent the crime and/or recover from its adverse effects. The aim of socio-emotional component is to provide students with identity awareness as cybercitizens, share values based on (cyber) human rights, develop empathy, solidarity and respect for the victims of cyberbullying, and feel responsible for cyber offence. The aim of behavioral component is to make people become aware of the ways they can avoid cyberbullying, help victims recover from pains of cyberbullying, educate peers about cyberbullying, and build a cyber-identity. A summary of the proposed program and its components are presented in Table 2.

Table 2. A cyberbullying prevention course for Iranian students

Content	Activities	Resources	Timeline
1. Concepts, Themes 2. Facts (statistics/true stories) 3. Laws and regulations 4. ICT literacy & Netiquettes	– Lectures – Reflections – Discussion – Interviews – Round table discussions – Talk show simulations – Self-assessment and needs analysis – Field trip to rehabilitation centers or (juvenile) prisons	Books, articles official reports, films, attendance of (relatives of) offenders/victims, United Nations human rights manuals, local legislations, handbooks, websites, mobile apps, software programs	- Two 90-minute sessions - Three 90-minute sessions - Five hours - Three 60-minute sessions

Concluding Statement

This paper addressed the concepts of cybercrimes and cyberbullying from a practical perspective considering a specific context, i.e., Iran. Iranian IT policy and cyber legislations were briefly reviewed and some suggestions

for the future to prevent cyberbullying and the safeguarding the cyber human rights were provided. Finally, some educational initiatives were discussed and a cyberbully prevention program was suggested for the Iranian situation.

References

Bhat, S., Chang, S., & Linscott, J. 2010. "Addressing cyberbullying as a media literacy issue," *New Horizons in Education,* 58(3), 34-43.

Brighi, A., Guarini, A., Melotti, G., Galli, S., Gena, A. 2012. "Predictors of victimization across direct bullying, indirect bullying and cyberbullying," *Emotional & Behavioral Difficulties,* 17, 375-388.

Jaghoory, H., Björkqvist, K., & Österman, K. 2015. "Cyberbullying among adolescents: A comparison between Iran and Finland," *JCALB,* 3(6), 1-7.

Iran's ICT Strategic Plan. 2007. Tehran: Higher Council of ICT.

Longman Dictionary of Contemporary English. 2010. UK: Longman.

Olenkin-Shemesh, D., Heiman, T., Eden, S. 2012. "Cyberbullying victimization in adolescents: Relationships with loneliness and depressive mood," E*motional & Behavioral Difficulties,* 17, 361-374.

Sahin, M. 2012. "The relationship between the cyberbullying/cybervictimization and loneliness among adolescents," *Children Youth Services Review,* 34, 834-837.

Sourander, A., Brunstein Klomek, A., Ikonen, M., Lindroos, J., Luntamo, T., et al. 2010. "Psychosocial risk factors associated with cyberbullying among adolescents: A population-based study," *Arch Gen Psychiatry,* 67, 720-728.

Tan, M., Park, J., Patravanich, S., & Cheong, J. 2014. *Fostering digital citizenship through safe and responsible use of ICT: A review of current status in Asia and the Pacific as of December 2014.* Thailand: UNESCO Asia-Pacific Regional Bureau of Education.

Ybarra, M.L. 2004. "Linkages between depressive symptomatology and Internet harassment among young regular Internet users," *Cyber Psychological Behavior,* 7, 247257.

Websites:

www.acorn.gov.au
www.caccollincounty.org/cyber-citizenship
www.cyber.polic.ir
http://data.un.org
www.stopbullying.gov
www.techopedia.com
www.techrasa. com

Endnotes

1 Online Longman Dictionary, www.ldoceonline.com/dictionary/bully.

2 Cyber-bullying, Australian Cybercrime Online Reporting Network (ACORN), www.acorn.gov.au/learn-about-cybercrime/cyber-bullying.

3 See Country Profiles, Iran (Islamic Republic of), Environment and infrastructure indicators, UN Data, http://data.un.org/en/iso/ir.html.

4 See the English version of 1404 Perspective Document in the website of Iran Social Science Data Portal, http://irandataportal.syr.edu/20-year-national-vision.

5 International Telecommunication Union (ITU), www.itu.int/net4/ITU-D/idi/2017/.

6 International Society for Technology in Education (ISTE), www.iste.org/standards.