



Journal of Emerging Trends in Social Sciences and Humanities

A Double-Blind, Peer-Reviewed, HEC recognized Y-category Research Journal

E-ISSN: [3006-7898](#) P-ISSN: [3006-788X](#)

Volume 3, Issue 2, 2026, 122-132



Social Media as a Threat to National Security: Assessing Human Security, State Regulations and Global Trends

Dr. Waseem Khokhar¹ Muhammad Shahroz Maalik²

¹ Assistant Professor, Department of International Relations, MY University, Islamabad, Pakistan.

² MPhil, International Relations, MY University, Islamabad, Pakistan.

Corresponding Author: Dr. Waseem Khokhar, **Email:** waseemkhokhar22@gmail.com

Article Information

Received:

2026-04-13

Revised:

2026-05-12

Accepted:

2026-06-16

Keywords

Social Media; National Security; Human Security; Pakistan; Australia; US; Visa Screening; Social Media Bans.

ABSTRACT

The role of social media in modern society is very important in defining the nature of politics, security and relationships within and among nations. Although social media encourages communications and innovations, yet such platforms create serious challenges to the national security and human security (Buzan, 1991; Buzan and Hansen, 2009). Acting negatively on these matters includes disinformation, recruitment, influence operations enabled by cyber capabilities, sensitive information reveal and manipulating people's mind initiated and spread through social media. In an attempt to address these new security challenges, countries have undertaken different strategies and policies such as banning the use of social media platforms, access restrictions based on the ages of people and also the social media reviews in the immigration or visa evaluation systems (Australian Government Department of Infrastructure et al., 2024; U.S. Department of Homeland Security, 2019; UNDP, 1994). The article critically evaluates the role of social media as a non-traditional threat to national security given the perspective of human security. The assessment consists of a critical evaluation of social media bans in Pakistan, their role in addressing national security and political stability in Pakistan, social media access restriction for children under 16 in Australia and Spain, social security of society in Australia and social media screening in work visa requirements in the USA under H1B visa requirements in America.

1. Introduction

The digital revolution has had great impact on the nature of security in this new millennium. Cyber social sites, which were considered a neutral platform for social interaction in the early days,

has emerged as a very potent tool having the capacity of influencing the political narrative-making people's behaviour and mass mobilising. Whether it is poll manipulation, recruitment of terrorists, cyberbullying or psychological



© 2026 by the authors. Licensee Khokhar & Maalik. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license <https://creativecommons.org/licenses/by/4.0/>

Publisher: Institute for Educating Environmental Resilience and Governance

operations, social media platforms have become an important space of contestation in national security (Bradshaw et al., 2021).

The traditional concept of national security was concentrated mainly on military security, territorial security and state survival. But with the onset of social media, new dynamic and non-kinetic threats have emerged and operate in a cross-border and social context, which are not accommodated into, or do not interact with, traditional defence systems.

However, social media has a simultaneous effect on human security which is a focus on protecting a person against fear, violence and vulnerability. The problem of online radicalization, the crisis of misinformation, cyberbullying and mental effects in children or adolescents can prove that the security in social media is not limited to the state level but can be measured on a personal level.

Nation states have also increasingly securitized social media through banning, regulation, surveillance and integration into visa screening programs. Pakistan's periodic banning of social media sites, Australia's prohibition on social media usage by people below the age of 16, and America's requirement of social media disclosure and screening in visa categories like H1B are all a part of this global trend to securitize social media (Freedom House, 2023).

The article covers the way the social media affects national security and where these problems intersect with human security and how governments respond to the effects of social media through control. A comparative analysis will be conducted to analyse the development of the regulation of social media at the global level.

2. Conceptual Framework National Security and Human Security

National security has traditionally been thought of as the protection of a state's sovereignty, political independence (Buzan, 1991). In this view, protection is mainly about the survival of the nation against external and internal threats, whether they come in the form of military aggression, political interference or internal disorder. As Barry Buzan (1991) explains, the state has historically been the essential item of security, and its institutions, borders and authority have been the number one cognisance of

protection. This state-centred understanding of protection began to change within the late 20th century - a new establishment of vulnerability was developed that could not be addressed fully via military or diplomatic implications.

This shift became especially apparent with the emergence of the concept of human security introduced through the agency of the United Nations Development Program in 1994 (UNDP, 1994). Human safety actions state that people are no longer really cosy simply because the USA isn't at war. Instead, security also relies upon whether and not individuals have access to food, healthcare, employment, political rights, personal protection and psychological well-being. Threats, combined with poverty, disorder, political repression, crime and social exclusion may be just as harmful to human life and dignity as armed conflict. Human protection therefore broadens the means of security to consist of economic, environmental, personal and political dimensions (UNDP, 1994).

In the modern-day digital age, social media has become a great pressure on national protection and human safety with complex and often contradictory effects. On one hand, those platforms offer spaces for the verbal exchange, political participation and the unfastened exchange of thoughts. On the other hand, they've opened up new vulnerabilities that can be exploited by state and non-state actors. From the perspective of state security, social media is now an important device in facts warfare. Governments, intelligence agencies and political groups can use online platforms to spread propaganda, manipulate public opinion, interfere in elections and deepen social divisions inside rival states (Rid, 2020; Wardle & Derakhshan, 2017). Disinformation marketing campaigns, faux news and coordinated online influence can undermine trust in democratic institutions, provoke unrest and destabilise societies without a single shot being fired.

Furthermore, social media has been used additionally with the aid of extremist and terrorist agencies to recruit supporters, spread ideological messages and raise funds and coordinate activities. These digital communities mean that such things can reach audiences some distance behind their physical locations, which makes them

more difficult for states to control or contain. Cyber activities consisting of hacking, statistics leaks and online sabotage also can threaten crucial infrastructure, communication infrastructure and government institutions (Weimann, 2015). In this way cyberspace has become an important battlefield in modern national safety strategy.

At the level of human security, social media is a different but identically extreme set of demanding situations. While it allows human beings to connect and express themselves, it leaves them vulnerable to harassment, cyberbullying, identity theft, misinformation and emotional damage. The constant stream of information, images and opinions can lead to a sense of anxiety, fear and confusion, especially as fake or fake information spreads quickly. Human beings may not be able to differentiate between truth and propaganda, which can undermine its ability to make knowledgeable decisions, including in politics, health or ultimate safety. Online abuse and specific harassment can be used to silence voices, damage the ideological basis and in extreme cases, even cause physical damage or self-harm.

Privacy is another main concern since social media gather substantial data of individual facts such as the region of users, possibilities, contacts and their behaviour (Couldry and Mejias, 2019). This information can be exploited for commercial profit, political concentration or surveillance. Individuals often have little control over how their statistics are saved, shared or used, which is a new form of vulnerability. As Buzan, Waever and de Wilde have argued, threats to personal security, privacy and the right of entry to reliable information should now be understood as part of the overall safety environment.

The tendency of state and human security overlapping in the digital world helps provide an explanation for why governments are increasingly intervening more in our online world. States insist that they must be able to modify social media to combat terrorism, interference from their overseas, cybercrime and disinformation. At the same time, they have the notion of protecting citizens from online harm, exploitation and abuse. But these types of interventions are often controversial and curb online content, expand surveillance, or limit access to positive platforms and thus can undermine freedom of expression,

political competition, and independent journalism. Measures taken for security reasons can also be used to repress dissent or control public debate.

As a result, social media has emerged as an arena in which the tradeoff between security and liberty is continually being negotiated. Governments are faced with the challenge of balancing the requirements of safeguarding the national balance and individual safety with the desire to uphold the democratic freedoms and human rights. This makes cybersecurity not only a technical challenge but a deeply political, social and ethical one. In the digital age, the future of national security and human security will depend on how societies are able to deal with this fragile balance between control and freedom, protection and rights, and kingdom electricity and personal autonomy (Buzan & Hansen, 2009).

3. Social Media: Threat to National Security

3.1 Disinformation & Information Warfare

Social media has enabled information to move at an unprecedented level, true or not. Content does not pass through the normal gatekeepers, such as editors or fact checkers, before it is available to the public. It is the algorithm that makes decisions about what to show and these algorithms are designed to prioritize material that comes with a lot of attention, emotion and engagement. This means that sensational content, polarizing and even inaccurate information circulates much faster and wider than balanced or carefully checked information.

This digital environment has led to the conditions for false information and information battles. State and non-state actors can deliberately change stories to influence public opinion, weaken trust in institutions and make social divisions worse (Buzan, B., 1991). Social media platforms are increasingly becoming tools for mind games; the objective is no longer always to convince people of one point of view, but to confuse them, provide them with too much information and have them highly disagree with each other. State actors and non-state actors employ the environment in spreading fake information and in information warfare (Wardle & Derakhshan, 2017). By bombarding users with conflicting claims, conspiracy theories, or emotionally evocative

stories, these operations make it more difficult for citizens to agree on the basic facts or to trust official sources.

Election periods of civil unrest and times of public health crisis have been particularly vulnerable to such campaigns. During elections, false or misleading stories about candidates or the process or alleged fraud can discourage participation or undermine confidence in democratic outcomes. In times of protest or political instability, online platforms can help amplify rumours, provoke anger and encourage confrontation. During public health emergencies, such as an outbreak of diseases, disinformation about vaccines, treatments or government policies can cost people's lives by encouraging them to ignore medical advice or reject lifesaving measures.

Modern information warfare is much more difficult to figure out than propaganda. This is because traditional propaganda is typically issued by state institutions that are easy to identify. On the other hand, the contemporary information warfare can be conducted by using fake accounts and anonymous users on the internet (Rid, 2020). Bots can also be used to spread information and can even be spread by ordinary citizens who do not know that they are spreading false information. Modern information warfare is difficult to trace, as many such online influence operations are cleverly disguised.

In this way, social media has changed the nature of the conflict. Instead of using only military power or official channels of propaganda, actors may now fight psychological and informational wars directly within the population of another country. This weakens national cohesion and undermines democratic processes leading to long-term instability and this is all happening in a way that is not very visible and hard to confront.

3.2 Extremism & Radicalization

Extremist groups are really good at using media to get their message out. They use Facebook, X, YouTube, Telegram and TikTok to reach a lot of people without having to spend money and take big risks. These groups create videos and posts to make violence appear sensationalized. They try to make people believe that what they are doing is heroic or is okay. They also disseminate ideas that appeal to people who are in any way complicated

by government/system. Extremist groups take advantage of the media to recruit people, make plans and get money (Weimann, 2015).

These online spaces are really strong because they do not just send out messages but they bring people together to create communities. People who embrace these groups are members of networks in which they hear the same extreme ideas, over and over. After a while this begins to seem the norm to them. They start to believe that violent talk is acceptable and this makes them feel like they belong to something and this could be more effective. In these spaces people who might never have met these extreme groups in real life can slowly start to think like them, thus making it easy for people to get pulled into the world of groups.

In countries, such as Pakistan, which have a great deal of security problems, social media helps terrorist and militant organisations get their message out. When issues and disagreements arise in religion or between the countries in these countries (Freedom House, 2023). This could lead people to believe that violence is an option to manage these issues.

Foreign and domestic extremist groups can also use media to convey specific messages to certain communities, which makes their messages more effective and allows them to reach more people. Online radicalisation has helped to lower the barriers to entry into extremist networks and the individual need not have direct physical contact with recruiters or training camps in order to be involved. Instead, they can progress from being passive consumers of extremist content to playing an active role through encrypted messaging apps, private channels and online fundraising platforms. This abrupt shift from the ideological level to the action level speeds up the process of radicalisation as it becomes more difficult for security agencies to detect, disrupt or prevent violent activities before they take place.

3.3 Disclosure of Sensitive & Ops Info

Social media is a problem when we speak of security. People can get themselves into trouble because they tell so much about themselves on the internet. For instance, individuals in the military and just regular people tend to post things about their lives online without really thinking about

potential exposure of sensitive information. These pictures and video can give away secrets about the military. For instance, they can indicate where the troops are moving to or where the military bases are situated. Such sensitive information is depicted in these pictures and videos that can indicate what the security forces are doing, where the security forces are.

So social media is a security risk because people give a lot about them and other people (Twenge et al., 2023). Something that does not seem like a deal on its own can become a big problem when social media is combined with other things that people can find online. The risks we face are bigger now due to the increased use of open source intelligence by more people. Open source intelligence (OSINT) means that our enemies including terrorists, criminal groups and spy agencies are looking at what we post on media to get most of their information.

Software tools are beneficial because they help people to keep track of the movements of people and institutions. These software tools figure out who is connected to whom and they find out weaknesses in individuals and institutions. The software tools are very useful in tracking the movements of individuals and institutions and identifying networks of individuals and institutions.

This means that social media is not just a platform for communication, it has transformed into a large and ever-changing database of intelligence. When people post personal or operational information online, they may be unwittingly contributing to the enhancement of the surveillance and targeting capabilities of hostile actors. In sensitive security environments, even slight lapses in digital discipline can therefore have serious real world consequences, including increased risks to personnel, facilities and civilian lives.

4. The Human Security Aspects of Social Media

National security is about keeping the country safe & stable. When people misuse media, then it hurts people personally. Things such as being harassed, seeing hate speech and being bullied on the internet. Having private information shared without permission really has an impact on people's sense of safety. People should be able to

use media without having to be bullied or having their private information shared. This is a part of national security, so people are safe from these kinds of things on the internet.

The bad effects of media misuse can last for a long time. It has an effect on people's well-being. Makes them feel unsafe. National security is important. Social media misuse is an issue that can make people feel really bad, so we need to think about social media misuse and how it hurts people. When bad information gets disseminated in times of an emergency, it really shows how people can feel insecure. If someone shares information about things like disasters, medical treatments or how to stay safe, people might do things that put them in danger (Howard & Hussain, 2013).

When you see a lot of hateful things online or things that are not suitable for everyone that can be really depraved for people's emotional health. This is especially true for people who are still growing and figuring out who they are. Seeing a lot of things online can be very upsetting for people's emotional health and yet it's even worse for young people who are still growing and trying to find out who they are as a person. The internet has a lot of things that are not suitable for everyone and seeing these things can be really bad for people's emotional health, especially for young people.

The problems which kids and teenagers face are really scary. Kids and teenagers spend a lot of time online with their friends that makes them targets for people who want to manipulate kids and teenagers or show kids and teenagers things that are not good for them. So social media algorithms are not good for kids because it shows them things that are scary. These algorithms cause kids to view stories over and over.

As a result, social media regulation is now coming to be viewed not just from the perspective of national security or censorship, but from a human security perspective also. Governments and societies are starting to understand that the protection of individuals against psychological harm, exploitation and digital abuse is a valid security issue (Poell & de Waal, 2018). From this perspective, regulation is not viewed as limiting the right to free speech, but instead as an urgent step to protect people's mental health and their

personal dignity and the safety of vulnerable populations in the digital age.

5. State Responses - Regulation, Bans and Surveillance

5.1 Pakistan: Social Media Ban, & Internal Security

Pakistan has frequently prevented people from using media websites such as TikTok and X, which was formerly known as Twitter (Bradshaw et al., 2021). This is because there are protests or the government is concerned about security. The government says that it does this in order to keep the country safe and in order to prevent people from maligning national cohesiveness. They also want to prevent people from spreading information that may enrage people or cause trouble. Pakistan does this for its protection and people's safety. The government blocks these media sites during trouble in order to keep order and ensure that everyone is safe. The government and Pakistan Telecommunication Authority take down a lot of accounts and posts that are associated with groups that are anti-government and harmful to the populace.

These bans are not good as they also have some downsides. When government restricts access to media it affects our freedom of saying what we think, ability to take part in politics and the work of journalist and to the economy especially to small business people, people who work for themselves and people who make content for the internet (United Nations Human Rights Council, 2011). When they persist in shutting down the internet and limiting access to it, it causes people to trust the government less. It creates less space for people to discuss important issues in a democratic manner. Social media is important for freedom of expression, democratic debate and restricting media can have serious consequences. Pakistan's approach to security is largely what the state wants. The government believes that it is more important to be in control and have stability than the people having rights on the internet. This means that digital rights and individual freedoms are not as important as being in charge to the government.

5.2 Australia: Social Media Laws for Children Under 16

Australia is an example of a different way of regulating social media. The main reason for this is not about keeping the country stable, instead the government in Australia is really worried about how the social media can hurt the younger population. There are a lot of problems with media, such as people being mean to each other online, mental health issues and kids being taken advantage of online presence.

Australia is looking at media as something that can affect people's health and safety especially young generation (Australian Government Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 2024). By doing this, they are changing the conversation, from stopping people from saying things, to making sure that people who are vulnerable are safe.

However, it is really hard to make sure people follow the rules especially when it comes to parents, schools and companies reporting on themselves. This new policy is a big deal because it changes the way we think about problems in the internet. It looks at safety as a way to make our whole community stronger not something the police have to deal with. This means we are trying to stop things from happening in the first place rather than just punishing people after something goes wrong. The policy is all about threats and online safety and it is good that we are taking digital threats and online safety seriously.

5.3 Spain Ban of Social Media for Children Under 16

Spain is another example of a country taking strong action to regulate how children use social media. The Spanish government is deeply concerned about the harmful effects that online platforms can have on young people's mental health, safety and well-being. Officials say that social media can expose children to danger such as cyberbullying, hate content and disinformation against Spanish government and law enforcement authorities.

The Spanish government has announced a plan to ban access to social media for anyone under the age of 16. Under this plan the most popular platforms like Facebook, Instagram, snapchat and others would have to introduce effective age-verification system to make sure that these kids

cannot create account independently. Because these platforms not only effect the behaviour of kids but also effect the mental health and safety of the new generation.

However, it won't be simple to enforce technical and privacy challenges specially verifying age without compromising users' data could make effective implementation difficult. Despite these challenges, many parents support stronger safety protection online. Survey indicates a large percentage of Spanish parents agreed with tighter restrictions to help keep children safer in the digital wild west, it reflects shifting focus to monitor problems to prevent them in the first place and protect the younger generation even better.

5.4 United States: Screening for Visa and Immigration using Social Media Policy

United States is doing things differently (U.S. Department of Homeland Security, 2019). It is using media to assist in immigration and visa decisions. People who want a visa now need to provide their social media accounts and information of media since last five years. For example, it is for work permits like the H-1B visa. The H-1B visa allows talented foreign professionals to work in the United States and wants to know about the media accounts of people who apply for the H-1B visa and other types of visas.

At the same time, civil liberties organisations have raised serious concerns around issues of privacy, discrimination and freedom of expression. Critics, however, say people might censor themselves online for fear and that their posts on social media could be misinterpreted by immigration officials. Nevertheless, this policy is part of a wider trend towards the securitisation of digital identity whereby online behaviour becomes part of border control and national security decision-making.

6. Case Studies

6.1 The January 6, 2021 U.S. Capitol Riot

The United States Capitol was stormed in January 6 2021 (Select Committee, 2022). This showed how big part social media played in helping real people get violent. People used the internet to spread lies of the election being fake. They used it to get their supporters pumped up and plan what they were going to do. On media people have

written posts, they talked in private groups and messaging apps. The storming of the United States Capitol was a result social media which helped people plan and get ready for this event.

Social media platforms are actually tools that help people recruit, plan and get ready for action. A lot of the people that were part of the riots got pulled into groups that kept telling them extreme ideas and encouraging them to fight against the government. This situation illustrates what occurs when social media platforms are used in the manner which they are meant to be free. It can cause a problem, of the whole country, and it does not even need to involve other countries. This teaches us the importance of information warfare within a country to make people lose faith in systems and lead to anarchy within the state. Information warfare is a problem. That can lead to large scale instability and can make people question everything resulting to cause instability.

6.2 Extremist Networks in South Asia

In South Asia social media is really important for the groups like extremists and terrorists. They use it to get more people to listen to them and to get power. These militant groups put their ideas on the internet, make violence look good and to find new people to join them without getting in touch physically. For instance, in Pakistan the government officials in charge of security have discovered social media accounts belonging to groups that are not permitted due to being engaged in terrorism and violence against certain groups of human beings. So social media is a tool that these extremist and terrorist organisations are using to spread their messages and get what they want.

It shows that extremist elements always find themselves a way to adjust. The internet is constantly shifting so extremist groups can re-emerge in numerous ways and means. This shows that it is not enough just react to the problem. We need to do more to stop these groups using the technology to gather information, and these groups from prospering.

6.3 Sri Lanka: Social Media Shutdowns After Easter Attacks (2019)

Following the terrorist attacks on Easter Sunday in April 2019 Sri Lanka had one of the deadliest incidences of radical ferocity in its modern antiquity. In the result, the social media setups

such as Facebook, WhatsApp, YouTube and Instagram were temporarily obstructed by the administration. The assessment was based after experts perceiving of a prompt blowout of fake narrative, provocative religious content and anecdotes that was driving terror, rage and the danger of religious infringement between religious elements.

The government claimed that these blackouts were necessary to prevent more discontent and potential punitive attacks. Sri Lanka has a past of racial and religious strains and social media had formerly played a part in intensifying hate and organizing uprisings. In this situation, the government considered digital platforms to be contributors of the volatility that could transform a single extremist outbreak into general social collapse.

However, the shutdown had also had serious human security consequences (Weimann, 2015). Citizens could not get access to reliable news, communicate with family members or even access online services, in a time of national emergency. Journalists, humanitarian organizations and regular people had difficulty sharing verified information, or counter rumours. This led to confusion, anxiety and in some cases panic, and illustrates how the restriction of digital communication can be harmful to individual safety and well-being even if the intention is to protect the stability of the nation.

7. Balancing Security and Freedom

The question is how to prevent people from actual dangers associated with social media while not undermining the very goods that make a country free and fair. Social media can be used to spread information, get people to believe in extreme ideas and plan violent acts. Iran has been a typical example of media use and misuse by the domestic and foreign elements. Peaceful protest leading to riots and acts of subversion and chaos by known and unknown components can proffer a classic example of the linkage between the "good and bad" of social media platforms (Howard & Hussain, 2013; Rid, 2020; Wardle & Derakhshan, 2017). Exacerbation of momentum of protests, as depicted by International and OTH media has envisaged a new fragment of threat for Iranian Islamic regime and thus considered to be a new domain of warfare.

Governance really is important in this regard. Evidences of current deplorable global situation suggests proactive and pre-emptive steps to cater for this very domain and needs to be balanced. We need to control media in a manner that is fair and clear. The rules for media should be easy to understand and predicated on laws not just decided on a megrim. Governments have to work with technology companies, people who watch about society and groups and can make sure the survival of governance is not hurt while keeping the true sense of liberty and freedom of expression. Social media needs to be regulated in a way that's transparent in its nature and commensurable.

The important thing is that we need to make sure that the mortal security is a part of our public security plans (Buzan et al. 1998). We shouldn't cover the country at the expense of the people living in it. When we make programs to stop risks, we have to make sure that they also cover people's internal health and their right to protection. And we also need to ensure that people are able to get the information they need and that they are free to say what they are supposed to say.

8. Conclusion

8.1 New Security Environment of Social Media

It is an element of maintaining a nation safe in the current world through social media. Our perception of safety was that of securing our country on the external front with police and armies. Now we know that is not enough. They exchange their minds and ideas with one another through media. Social media can alter the way individuals' view their government and their leaders and that is why it is a potent force in general security sphere. Media is also something about which we need to be cautious since it can work against us in case of not being careful. Social media is an offer and we cannot ignore it.

The various approaches that the countries take aim the result that there is no single approach in dealing with this issue. Almost every nation does what it believes is best depending on its manner of conducting politics how general populace is adaptive and what is initially perceived to be of utmost importance. Taking the case of Pakistan which is indeed concerned with preventing terrorism, Australia which is more concerned

about the safety of the young generation, and The United States which is screening the immigrants and job seekers using technology. Keeping in view the national interests, all these nations have notions of what it would mean to be safe at the internet and computers.

8.2 Appeals of Bans and Survey

As demonstrated in this paper, we cannot always rely on bans, shutdowns or surveillance to address threats. Such things may be useful temporarily in the case of a large scale problem, but in the long run it can result in so much damage. They cause people to lose trust in the government and restrict their expression of the way. Therefore, it may have serious negative impact on economy and lives of peoples. Censorship only removes the evidence of bad material; it does not eliminate the bad material. And when we monitor all of us all the time we may end up policing people as opposed to protecting them.

We are living in a world where everybody is intertwined. This implies the fact that it is extremely difficult to prevent the transmission of information. When a person attempts to dictate what people can see or do on the web by being strict or limiting them it typically does not. We should strengthen our communities to ensure that they are able to cope with arising problems. Security in the age is concerned with ensuring individuals and communities are able to manage hard situations. It is this that we refer to as security and safety of digital space.

8.3 The Significance of Human Security

The key argument in this paper is that national security and human security are truly interrelated

at this point. Social media not only influences the nations, but influences individuals as well. It may damage mental health of people, their privacy and self-respect. It goes as far as influencing the information that can be obtained by people. Cyberbullying, fake news, radicalisation on the internet and mind games make societies vulnerable.

Even when policies ensure that the country is safe, they may create issues when they fail to consider how they impact people. To be truly safe in the new world, we must secure people, in particular, children and the young generation that is more likely to be the victim of the abovementioned cyber threats. Teaching on a fundamental level, and motivating the people by the power to personalities and a set of rules that foster freedom, can bring a lot to the modern world of the constantly threatening global arena. We should educate individuals on the internet on how to use it in a safe manner. Narrative of protective regulations under the care of skilled authorities and regulatory legislations is obligatory to be transmitted in an appropriate way.

8.4 Towards a Balanced Digital Security Strategy.

They require the governments to balance between regulating the work of media and technology companies and educating people on the issues and ensuring the law regulates all. The best weapon against information warfare, extremism and online harm is a resilient society, that is, an educated, digitally aware, and socially cohesive society. In the virtual world, control does not suffice to give the country a long-term security but participation and preservation of human dignity.

Conflict of Interest

The authors showed no conflict of interest.

Funding

The authors did not mention any funding for this research.

References

- Australian Government, Department of Home Affairs. (2025). Online safety reforms and age-based restrictions on social media use. *Canberra: Commonwealth of Australia*.
- Australian Government, eSafety Commissioner. (2025). Protecting children from online harm: National online safety strategy. *Canberra*.
- Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. *Boulder, CO: Lynne Rienner Publishers*.
- Counter Extremism Project. (2025). The use of social media by extremist and terrorist organizations. Retrieved from <https://www.counterextremism.com>
- Freedom House. (2025). Freedom on the net 2025: The global drive to control big tech. *Washington, DC*.
- International Crisis Group. (2025). Information warfare and internal stability in South Asia. *Brussels*.
- Pakistan Telecommunication Authority. (2025). Annual report on content regulation, platform compliance and national security. *Islamabad: Government of Pakistan*.
- Reuters. (2025). Pakistan tightens control over social media amid security and political concerns. *Reuters News Agency*.
- Reuters. (2025). Australia moves to restrict social media access for children under 16. *Reuters News Agency*.
- United Nations Development Programme (UNDP). (1994). Human development report 1994: New dimensions of human security. *New York: Oxford University Press*.
- United Nations Office of Counter-Terrorism. (2025). The misuse of social media for terrorist purposes. *United Nations*.
- U.S. Department of Homeland Security. (2025). Social media screening and immigration vetting practices. *Washington, DC*.
- U.S. Department of State. (2025). Expanded screening and vetting for nonimmigrant visas, including H-1B. *Federal Register*.
- U.S. Government Accountability Office. (2025). Border security: Use of social media data in visa adjudication. *Washington, DC*.
- World Economic Forum (WEF) (2025). Global risks report 2025: Misinformation, cyber insecurity and state stability. *Geneva*.
- Zuboff, S. (2025). Surveillance capitalism, social media, and national power. *New York: Public Affairs*.
- Couldry, N., & Mejias, U. A. (2019). The costs of connection: How data is colonizing human life and appropriating it for capitalism. *Stanford University Press*.
- Bradshaw, S., Bailey, H., & Howard, P. N. (2021). Industrialized disinformation: 2020 global inventory of organized social media manipulation. *Oxford Internet Institute*.
- Buzan, B., & Hansen, L. (2009). The evolution of international security studies. *Cambridge University Press*.
- Howard, P. N., & Hussain, M. M. (2013). Democracy's fourth wave? Digital media and the Arab Spring. *Oxford University Press*.
- Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. *Lynne Rienner Publishers*.
- United Nations Development Programme. (1994). Human development report 1994: New dimensions of human security. *Oxford University Press*.

- Van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford University Press.
- Buzan, B. (1991). *People, states and fear: An agenda for international security studies in the post–Cold War era* (2nd ed.). Lynne Rienner Publishers.
- United Nations Development Programme. (1994). *Human development report 1994: New dimensions of human security*. Oxford University Press.
- United Nations Human Rights Council. (2011). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/17/27)*. United Nations.
- Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking*. Council of Europe.
- Weimann, G. (2015). *Terrorism in cyberspace: The next generation*. Woodrow Wilson Center Press.
- Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.
- Twenge, J. M., Haidt, J., Joiner, T. E., & Campbell, W. K. (2023). Social media use and mental health: A review. *Current Opinion in Psychology*, 52, 101574.
- Freedom House. (2023). *Freedom on the Net 2023: Pakistan*. Freedom House.
- Australian Government Department of Infrastructure, Transport, Regional Development, Communications and the Arts. (2024). *Age assurance trial for social media: Protecting children and young people online*. Australian Government.
- U.S. Department of Homeland Security. (2019). *Notice of information collection: Supplemental questions for visa applicants (84 Fed. Reg. 37301)*. Federal Register.
- Select Committee to Investigate the January 6th Attack on the United States Capitol. (2022). *Final report of the Select Committee to Investigate the January 6th Attack on the United States Capitol* (H. Rept. 117–663). U.S. Government Publishing Office.
- Weimann, G. (2015). *Terrorism in cyberspace: The next generation*. Woodrow Wilson Center Press.
- Reuters. (2026). *Spain to ban social media access for under-16s, PM Sanchez says*. Investing.com.