June 2026

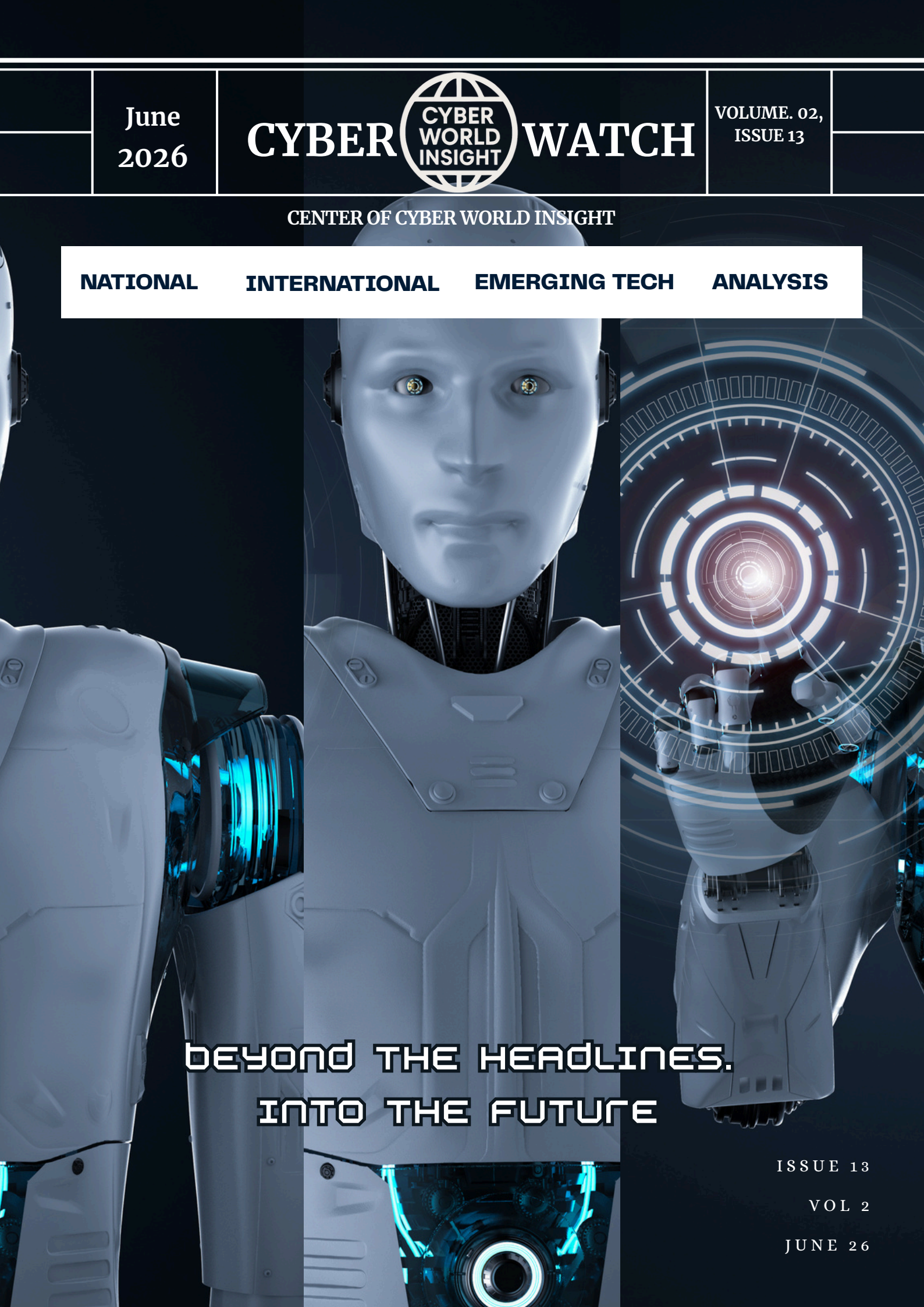
CYBER WATCH

CYBER WORLD INSIGHT

VOLUME. 02, ISSUE 13

CENTER OF CYBER WORLD INSIGHT

NATIONAL INTERNATIONAL EMERGING TECH ANALYSIS



BEYOND THE HEADLINES. INTO THE FUTURE

ISSUE 13

VOL 2

JUNE 26

June 2026

CYBER WATCH

VOLUME. 02, ISSUE 13

CENTER OF CYBER WORLD INSIGHT

June, 2026

About

CyberWatch is a policy and op-ed e-paper dedicated to exploring how technology is transforming Pakistan's society, economy, and governance. We bring together voices from academia, industry, and policy to debate the opportunities and risks of the digital age. Our mission is to inform, challenge, and shape the national conversation on Pakistan's technological future.

Publishing Information

Center for Cyber Research and Artificial Intelligence (CCRAI)©2023–2025
The Center for Cyber Research and Artificial Intelligence Pakistan
Office #401, Omega Heights, E/11-3,
Islamabad, Pakistan
🌐 Website: www.ccrai.org.pk
📧 Email:
news@cyberworldinsight.com
📱 Phone/WhatsApp: +92 333 5221408

Digital Edition

This is the Fortnightly Digital Edition of Cyber Watch.
📲 Available online at:
🌐 www.cyberworldinsight.com/cyberwatch
📥 Downloadable in PDF format for offline reading.

June 2026

CYBER WATCH

VOLUME. 02, ISSUE 13

CENTER FOR CYBER WORLD INSIGHT

June, 2026

FROM THE TEAM

Cybersecurity, artificial intelligence, and emerging technologies continue to redefine the global digital landscape. As cyber threats become more sophisticated and AI accelerates both innovation and risk, governments, businesses, and institutions are placing greater emphasis on digital resilience, secure infrastructure, and responsible technological advancement.

In this issue of CyberWatch, we examine some of the most significant developments shaping today's cyber ecosystem. From CISA's decision to shorten critical vulnerability patching timelines in response to AI-driven threats to Pakistan's position in the Global Cybersecurity Index, we explore how cybersecurity is increasingly becoming a matter of national resilience rather than merely technical defence.

Beyond reporting the latest developments, this edition seeks to provide context, analysis, and practical insights into the evolving intersection of cybersecurity, artificial intelligence, technology, and international affairs. As digital transformation accelerates, understanding both the opportunities and the challenges of emerging technologies has never been more important.

We hope this issue offers our readers valuable perspectives on the rapidly changing cyber domain and contributes to informed discussions on building a safer, more resilient digital future.

Finally, we extend our sincere appreciation to our contributors, editorial team, and readers for their continued support and commitment to advancing cybersecurity awareness and knowledge.

Editor-in-Charge, CyberWatch E-paper,
Center for Cyber World Insight

Kainat Shahid

THE WAIT IS OVER!

YOUR JOURNEY STARTS NOW

CYBER WORLD INSIGHT

CENTRE OF CYBER WORLD INSIGHT (CCWI)

RESEARCH • ANALYZE • EMPOWER

Be part of a **purpose-driven** internship that builds **skills**, inspires **impact** and shapes the **future**.

BATCH-II

SUMMER INTERNSHIP PROGRAM 2026

INTERNSHIP OPPORTUNITIES

RESEARCH DIVISION
Dive deep into research, analyze global issues and contribute to insightful reports.

CONTENT WRITERS DIVISION
Craft powerful articles, blogs and reports that inform and influence.

NEWS SECTION
Stay ahead. Report right. Be the voice of truth and awareness.

GRAPHIC & VIDEO DIVISION
Design visuals that speak. Create impactful graphics and videos that inspire.

CYBER SECURITY DIVISION
Explore, learn and strengthen the digital world through cyber defense.

ELIGIBILITY CRITERIA

For Research Division & Cyber Security Division

Minimum Qualification (at least):

- BS in Computer Science (CS)
- International Relations (IR)
- Defence & Strategic Studies
- Peace & Conflict Studies (PCS)
- Governance & Public Policy
- Or related disciplines

IMPORTANT DATES

LAST DATE TO APPLY
JULY 10, 2026

INTERNSHIP BEGINS
JULY 20, 2026

HOW TO APPLY?

1. Send your CV to
   hr@cyberworldinsight.com
2. Fill the Internship Application Form

SCAN QR CODE OR VISIT LINK BELOW

APPLY TODAY.

WHY JOIN CCWI?

- Work with experienced researchers and professionals
- Develop practical and professional skills
- Enhance your research and analytical capabilities
- Build an impressive portfolio
- Expand your professional network
- Receive a Certificate of Completion
- Opportunity to become part of future CCWI projects

DON'T JUST WATCH THE FUTURE–
HELP SHAPE IT.

LEARN. RESEARCH. CREATE. INNOVATE. LEAD.

June 2026

LATEST CYBER NEWS

VOLUME. 02, ISSUE 13

CYBERATTACK DISRUPTS BANKING SERVICES ACROSS THREE MAJOR IRANIAN BANKS

A synchronized cyber attack on three major financial institutions in Iran, Bank Melli, Bank Saderat and Bank Tejarat, was confirmed by the Iranian authorities, resulting in the temporary suspension of card based banking services. The attack had an impact on ATM withdrawals, point-of-sale payments and mobile banking transactions, leading to a temporary cessation of some ATM services and efforts by other cybersecurity mechanisms to contain the attack. Authorities said that no customer money had beentouched and restoration work had started. The incident comes after a cyber attack earlier this month that was reported as a disruption of financial services, adding to a series of cyber tensions exchanges throughout the region. Analysts note that financial institutions are still considered one of the most appealing targets for threat actors, whether state sponsored or financially motivated. This is due to their essential importance to the economy and the security of a nation.

(Source: Reuters , 2026)

June 2026

LATEST CYBER NEWS

VOLUME. 02, ISSUE 13

MICROSOFT ADDRESSES RECORD 206 SECURITY VULNERABILITIES IN JUNE PATCH TUESDAY

Microsoft's June 2026 Patch Tuesday addressed 206 security vulnerabilities, making it one of the company's largest monthly security updates on record. Three vulnerabilities were actively known and have been addressed in the release, continuing Microsoft's commitment to the security of Windows and enterprise operating systems. Security experts are urging organizations to prioritize installation of the updates, especially for networks that are exposed to the internet and enterprise environments. Experts have suggested that before an organization patches an application fully, it should first test the patch on those systems that are actually critical to the business and not delay the process of patching that allows an organization to be vulnerable to exploitation.

(Source: Hacker Storm , 2026)

June 2026

LATEST CYBER NEWS

VOLUME. 02, ISSUE 13

CISA Tightens Patch Deadlines as AI Accelerates Cyber Threats

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has introduced a new directive requiring federal civilian agencies to remediate the most critical cybersecurity vulnerabilities within three days. The updated policy reflects growing concerns that cyber threat actors are increasingly leveraging artificial intelligence to identify, develop, and exploit vulnerabilities at unprecedented speed, significantly reducing the time organizations have to respond.

Previously, federal agencies often had several weeks to deploy security patches depending on the severity of a vulnerability. Under the revised guidance, agencies must patch, remove, or otherwise mitigate affected systems within a much shorter timeframe to reduce the risk of compromise. The directive aligns with CISA's broader efforts to strengthen cyber resilience and minimize opportunities for attackers targeting critical government infrastructure. Cybersecurity experts believe the accelerated patching requirements acknowledge the changing threat landscape, where AI-assisted reconnaissance and automated exploitation are making cyberattacks faster and more sophisticated. Organizations are therefore being encouraged to improve vulnerability management, automate patch deployment where possible, and maintain continuous monitoring of internet-facing systems.

(Source: CISA, 2026)

June 2026

LATEST CYBER NEWS

VOLUME. 02, ISSUE 13

RANSOMWARE ATTACKS ACROSS EUROPE RISE MORE THAN 55%

Ransomware attacks against European organizations rose 55.1% YOY during the first four months of 2026, according to a new Cyber risk analysis. An average of 171 publicly disclosed attacks were observed per month and targeted such industries as health care, manufacturing, financial services, and government services. The report states it is partly due to the growth of automated attacks and ongoing strong performance of ransomware-as-a-service operations, as well as slower patching rates among some organizations. Effective countermeasures against the increasingly complex threats include employing robust backup strategies, using multi-factor authentication, training employees about security, and implementing prompt vulnerability management.

(Source: Infosecurity Magazine, 2026)

June 2026

CYBER REPORTS

VOLUME. 02, ISSUE 13

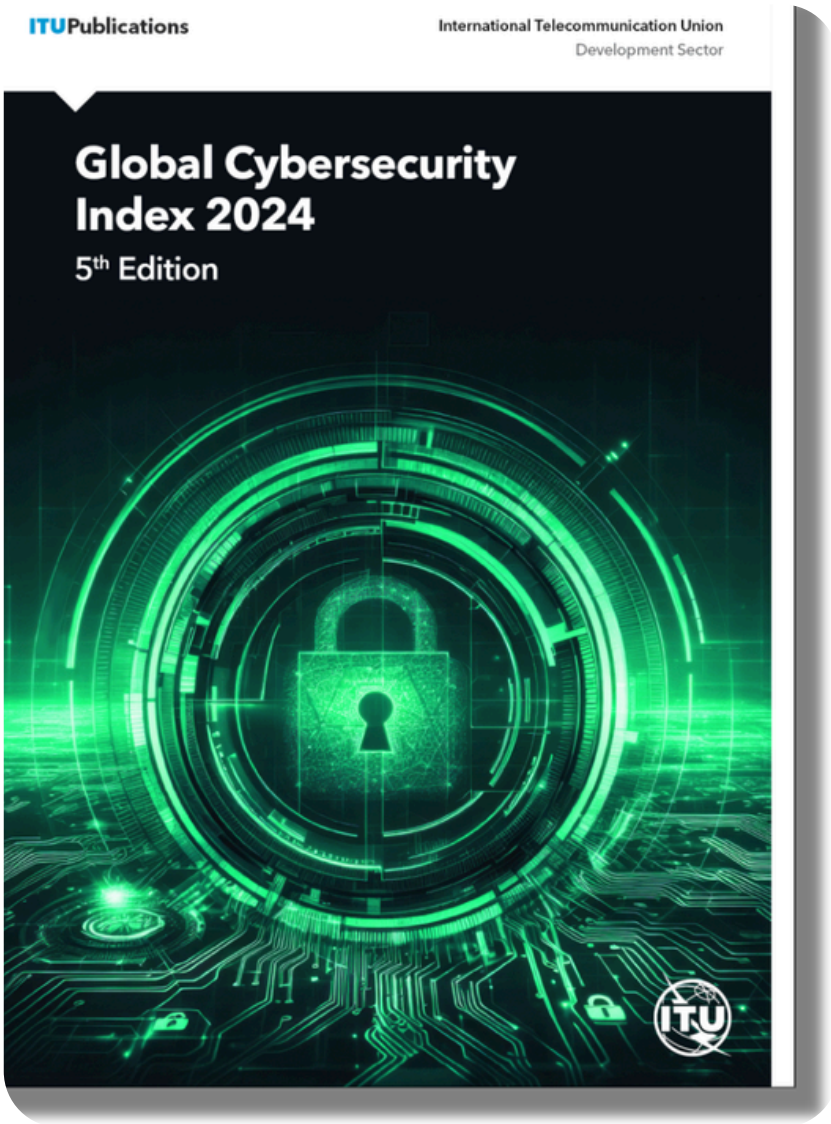
PAKISTAN RANKED 79TH IN THE GLOBAL CYBERSECURITY INDEX: WHAT THE NUMBER HIDES

Rank
79th

Assessment Areas
Legal, Technical, Organizational, Capacity Development, Cooperation

Key Challenge
Implementation and cyber capacity

Key Opportunity
Workforce development and stronger public-private collaboration



Pakistan's ranking of 79th in the Global Cybersecurity Index (GCI) is often cited as a measure of the country's cybersecurity readiness. While rankings offer a useful snapshot, they tell only part of the story. The bigger question is not Pakistan's position in the list, but what are the remaining factors influencing Pakistan's cyber resilience.

The GCI assesses countries on a number of aspects such as legal, technical capacity, organisation, capacity development, and international cooperation. In recent years, Pakistan has also taken significant strides forward with the creation of the National Cyber Emergency Response Team (National CERT), a focus on digital governance, and working to bolster cybersecurity legislation. The developments bear witness to the increasing importance given to cybersecurity as a national concern.

An increase in attack surface across the country has been brought about by the rapid digitalisation of the country, where digital banking, e-governance services, cloud, and online businesses are becoming hot targets for cybercriminals. Organizations including small and medium-sized businesses (SMEs), educational institutions and healthcare providers, may not have the financial means or technical resources to implement a well-rounded cybersecurity solution.

Meanwhile, public awareness of cyber security is far from uniform, and people continue to be targeted by phishing sites, online fraud and social engineering.

The ranking also does not adequately represent reality. Cyber maturity relies on policies and laws, but also on successful implementation, securing qualified human resources and responding to incidents as well as collaboration between government, industry and academia. As Pakistan's digital economy expands, ongoing investment in cybersecurity education, professional training, and the sharing of threat intelligence will be vital.

In coming days, Pakistan will have a chance to boost its ranking and cyber-resilience. Steps towards bolstering critical infrastructure protection, fostering public-private collaboration, nurturing cybersecurity start-ups, and cyber awareness can lead to a more secure digital environment. The Global Cybersecurity Index is not a scorecard, but a way to identify strengths, fill gaps and gauge long-term progress, which should be done by policymakers and organizations.

In the end, there's no clear-cut "best" or "worst" in terms of cybersecurity ranking. It's quantified through the capacity of a country to predict dangers, secure digital resources, react appropriately to incidents and build trust in a ever more interconnected world.

June 2026

AI ACROSS DISCIPLINES

VOLUME. 02, ISSUE 13

ONLINE HARASSMENT AND THE LAW

BY HADIA SARWAR

Cyber harassment is a crime against women, which is the most highlighted crime in contemporary times. Violence of any nature and form against women is unacceptable, and irrespective of the socioeconomic and social concerns. According to the account of Ban Ki-moon, who is a former United Nations Secretary-General, enunciated in 2008 that,

'There is one universal truth applicable to all countries, cultures and communities: Violence against women is never acceptable, never excusable and never tolerable. '

The internet was once a space of freedom, where people were free to express themselves, connect with others, and participate in social discussions without any fear. However, unfortunately for women, these platforms are a digital way of harassment. From leaking their photos to body shaming them, stalking them, and even threatening them. Digital violence against women has become the most underrated issue that is faced by almost every female. What makes this problem more challenging and troubling is not just the existence of digital violence, but the way it is being frequently repeated and ignored by the authorities. And females are mostly told to 'ignore it' or even 'stop posting on social media'. As all this is their fault, the question is, why are women wrong? Why does no one question the real victim or harasser?

Moreover, now this online harassment is not limited to influencers only. In fact, teenagers, ordinary women and even journalists are being victimised every day. Even if a female is posting her opinion on politics or rising voice against the wrong may receive rape threats. Similarly, if a teenage girl refuses to do something wrong in digital platforms can become the victim of false accounts and photoshopped images. These issues may seem small on screen, but those who are going through all this are well aware of the damage they face mentally and even physically. Most of the harassers may do these things for fun, but things they do for only fun can give someone a lifetime trauma.

Additionally, most women fear that reporting these harassment issues will just make things worse for them and their support may be less and they will face public shame. And this is the dark reality of the society we are living in, here the target chose silence over justice just to avoid society blames and drama.

In countries like Pakistan, awareness of cybercrime has increased, significantly with the introduction of institutions such as the Federal Investigation Agency cybercrime wing. Still the tariffing fear of social judgment is way stronger than the voice and hope of legal protection. Additionally, harassment and violence against the female is mostly normalized by making memes on it and even making it trend online and this normalization creates an environment where digital violence and harassment is no longer to be seen as an illegal act. In fact it's not even shocking anymore in our environment. Civil early the impact of this negative environment can create a very negative and uncomfortable future for the next generations. At this point women should take a stand on their own and should not disappear from their social circle just because of this violence in fact, they should stand and speak up for their rights.

The law serves as the backbone of every state conducive to creating balance in society. Multiple laws exist in Pakistan pertinent to women protection. However the main question is to what extent these laws are being implemented and contributing in taking action against this crime. Here, an important question remains that in the world where a significant amount of life exists digitally in this environment, if a female is not safe and if she cannot get comfortable in her digital space, can we really call that platform free for everyone?

June 2026

AI ACROSS DISCIPLINES

VOLUME. 02, ISSUE 13

Deepfakes and Electoral Integrity: How Synthetic Media Threatens Democratic Processes

BY NIQAB SHAHEEN

Introduction

The rapid growth of artificial intelligence technology has caused serious concerns for democracy in recent times because of the creation of deepfakes and fake news. As these tools become easily accessible, the process of consuming information undergoes fundamental changes. In this modern era, technological developments are taking place like never before, giving rise to various benefits as well as drawbacks. The greatest debate triggered by technological innovations in recent years is the creation of deepfakes, which are artificial intelligence videos, sounds, or pictures that appear incredibly realistic but are entirely fictional. Although there are several benefits of deepfakes, their misapplication may result in issues for democracy, particularly in elections.

Deepfakes are generated using complex algorithms within artificial intelligence, particularly machine learning, which analyse the behaviour and actions of actual people. These algorithms can generate synthetic media that imitates actual people with great precision. In this case, a deepfake video could feature a political figure giving a speech that they did not give. It would be difficult for most viewers to differentiate between fake and authentic media. The use of such technologies makes the election period very risky since information is essential for effective decision-making.

Misinformation and Electoral Manipulation

The very first issue related to deepfakes lies in the fact that these videos contribute to misinformation campaigns. An election campaign is one of the times when every single bit of information matters a lot. A video posted only a couple of days or even hours before the voting can claim that the candidate is involved in some form of criminal activities or has made some questionable remarks. This might lead to a situation where even after finding out the truth about the video being fake, the voters will never be able to change their minds.

Furthermore, deepfakes can distort public perception. The use of deepfakes can involve the production of emotionally loaded messages targeting communities or groups. Deepfakes may be tailored to generate negative emotions like fear or anger in certain voters based on cultural and political differences. Such constant exposure to these kinds of images and messages can influence people's attitudes even unconsciously. The manipulation involved in deepfakes destroys election fairness because voters make decisions based on artificial rather than real information.

In the US, India, Slovakia, and Brazil, simply the threat that damaging videos or remarks may be deepfakes enabled politicians to discredit their critics before they even started, while regular people withdrew into echo chambers or gave up.

Epistemic trust is not something that must be destroyed to have consequences it is a slow corrosion of the basis of democracy that transforms the act of voting from an exercise of popular sovereignty into a spectacle where the winner is always in doubt. Conceptually, the problem is not technological but deeply political: generative AI has used the gap between perception and reality to manipulate the way human cognition works, something that simple disinformation has never managed to do. The danger

that lies ahead is a crisis of legitimacy in democracy that cannot be resolved by any one election. The next serious issue related to the problem under discussion is the weakening of trust. The whole democratic system relies on people's trust in elections, media, and other aspects of politics. In this situation, the omnipresence of deepfakes raises concerns related to determining what is true and what is a fabrication. Eventually, it results in growing distrust in any information that one can come across. One is likely to become suspicious of news pieces and even videos, thinking that anything can be forged.

Deepfake threats are also more pronounced in countries where there are low levels of digital literacy among the general population. In such cases, the population lacks the knowledge on how to check the validity of information. The influence of social media in the spread of the deepfake issue is immense in such societies. Social media algorithms give priority to sensational and shocking news, thus enabling deepfakes to be shared rapidly within short periods.

The issue of tackling the problems that come with the use of deepfakes involves collaboration among various entities. First, technology firms should accept the blame by designing software that is able to recognize and classify the deepfakes. The artificial intelligence itself may also be deployed to distinguish any differences within the video footage such as unusual facial movements and inconsistent audio. The government should also provide legislation in the form of laws to regulate deepfakes in times of elections. On the other hand, public education is just as necessary. People need to be aware of the animation of deepfakes, and the possible danger associated with them. Media literacy enterprises will aid in ensuring that people are sceptical of any information they receive and are able to verify their sources before posting anything on social media.

Conclusions

The increase in cases of deepfakes and artificial intelligence-created synthetic media in the global election cycle has highlighted a crucial vulnerability within the structure of modern-day democracy – the susceptibility of the common perceptual reality that is shared by people. Although there has been little electoral interference by virtue of stable voter turnouts and minor shifts in votes caused by fake media, the impact has been more evil through psychological and epistemological means. For citizens from both mature and new democracies, the information environment today consists of a reality in which the credibility of visual and auditory evidence is no longer unquestionable. The liar's dividend has evolved into an overarching attitude of suspicion that invalidates not just disinformation but authentic information as well, thus forming a cycle of skepticism, distrust, and detachment from the process. The deepfake technology can also be regarded as one of the most effective means that come with pros and cons in today's world. Even though this technology offers numerous possibilities, it is important to acknowledge that the misuse of deepfake technology can result in serious problems concerning the credibility of the election process. The application of deepfake technology in spreading information and influencing the public opinion poses a serious threat to the stability of the election process.

June 2026

AI ACROSS DISCIPLINES

VOLUME. 02, ISSUE 13

Generate AI

GENERATIVE AI IN THE NEWS ROOM : TOOL OR THREAT TO THE JOURNALIST?

BY AYESHA ASIF

Technology has forever changed the newsroom. From typewriters to computer systems, from bulletin boards to digital mediums, journalism has been adapting along the way. Now, yet another revolution awaits at the doorstep of media houses worldwide – Generative Artificial Intelligence (AI). From ChatGPT to Gemini, image and video generators, AI systems are quickly making their way into the newsroom, posing the question: is generative AI a helpful tool for journalism or a danger to the craft itself?

Generative AI is defined as the ability of technology to produce human-like outputs, including writings, summaries, visuals, scripts, headlines, and audio files. Media outlets have begun adopting it for their benefit already. The application may include the production of summaries, creation of headlines, translations of writings, and assistance in data analyses. Meanwhile, there are those who are cautious due to the potential of AI to harm journalism practices, employment prospects, and the rapid proliferation of false information.

Advocates for AI believe that AI is a revolutionary technology that will revolutionize journalism and increase efficiency. Contemporary newsrooms operate in stressful conditions, where reporters have to produce stories fast without sacrificing their quality and accuracy. The use of AI can help reporters complete the routine tasks, which will enable them to spend more time interviewing people, conducting investigations, and telling a story. In this way, AI can be used to transcribe an interview, summarize public documents, or translate data into human language.

AI-generated reports have become common

practice in sports journalism and financial news. The report on the game or market trends can be generated automatically seconds after the event. Humans can then modify the text accordingly. In this case, the role of artificial intelligence will only be that of assistance in the production process rather than substitution.

Another benefit of generative AI is availability. Small news agencies can use AI technologies despite having a limited number of employees and funds. AI can be used for translating stories into other languages. This will allow journalists to target international audiences. Generative AI can actually promote journalism in underdeveloped countries by helping overcome language barriers.

Nevertheless, one should not overlook the potential risks connected with the development of AI for journalism. In no way is journalism limited to fast word creation. Journalism requires the truth, responsibility, and ethical standards, as well as other qualities that are completely alien to machines. The fact is that AI creates content through patterns of existing data. AI does not feel either moral norms, emotional states, or their consequences in social life. This means that AI is able to create distorted, biased, and even false content, sounding quite real.

This threat is probably the biggest challenge for contemporary journalism: the issue of disinformation. Fake news is currently a real issue, especially on the Internet. In this situation, the use of generative AI will only aggravate the problem by generating realistic pieces of content, including videos, images, or even false audio clips. To illustrate, one can mention the phenomenon of Deepfake. In some cases, Deepfake is able to replicate real individuals so realistically that distinguishing truth from falsehood becomes extremely difficult.

Journalists may lose their jobs since media outlets will try to save money and cut costs. They will need fewer employees to create content for their websites and publications, relying instead on the use of AI, which is much cheaper and quicker. As a result, young journalists who want to join the industry can be left without a job.

Additionally, AI relies on data provided by journalists, using information published on the web without their explicit permission or any compensation. Writers and reporters believe that AI enjoys the benefits of creativity while at the same time destroying its source.

Another aspect worth considering is the potential for bias. AI technology may work based on biased data sets, which may result in news articles carrying prejudice of a political, cultural, or social nature. Journalists have to produce unbiased articles, but there is no way for AI to independently check the ethical value of what it produces.

On the other hand, the rejection of AI technology might not be the best idea, as well. It often happens that technology becomes an integral part of society even if people reject it at first. For instance, many objected to the existence of the printing press, radio, television, or even the Internet when they appeared. The question is not whether there should be AI in newsrooms, but how it should be used.

First of all, media companies need to introduce strict regulations regarding the use of such technology. The AI-generated article still needs to undergo verification by human editors. Furthermore, readers have to be informed of any contribution made by the technology in producing an article or picture. Last but not least, newsrooms should develop digital skills among journalists to learn about AI's advantages and limitations.

It is also essential for educational establishments to take part in addressing the issue. Alongside learning how to conduct investigations and prepare a report, students need to study media ethics, fact-checking, and AI. The future journalist needs to learn how to work with the machine but

but not forget about human values in reporting.

In conclusion, generative AI is not a miracle or a monster. This is simply a tool that can either benefit journalism greatly or harm it immensely. When used properly, AI technology can help journalists to become faster, to enhance their research capabilities, and get more information. When misused, it may ruin the reputation of journalism, promote lies, and devalue the profession.

However, the fate of journalism has never been in the hands of technology alone. The success of a journalist depends on integrity, professionalism, and willingness to uncover the truth. While machines will be able to produce reports, they will never substitute human moral standards. In the end, journalism can be successful only when human values remain important.

June 2026

AI ACROSS DISCIPLINES

VOLUME. 02, ISSUE 13

SMART HOME / IOT TECH ADOPTION IN ZIMBABWE

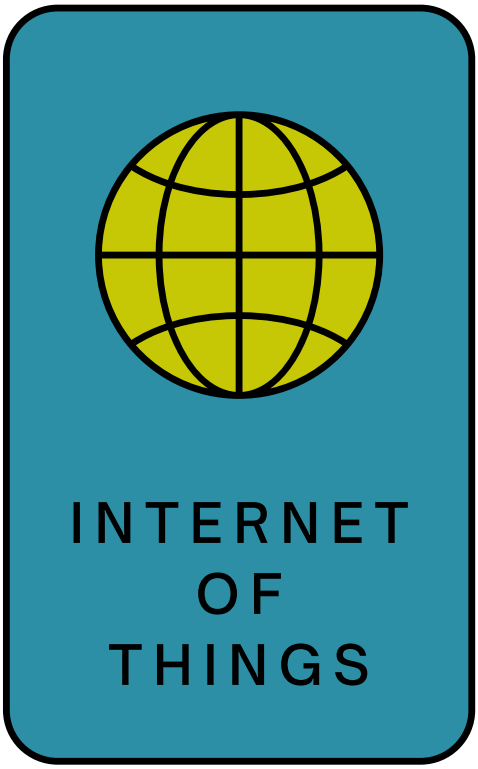
BY GODFREY MASAWI

Technological advancement has been on the rise across the globe, and also in Africa, in particular, Zimbabwe. The government has advocated for the increase and adoption of smart technology amongst many people so as to fast-track development through digitalisation. This digital transformation has always led to a better way of doing business and enhancing the livelihoods of many people, particularly the youth Internet exposure has led to many people having a better world view, and this has improved their social standing as well. Smart Home adoption has helped bridge the gap between the rural and the urban population for many people.

Through the Look East policy adopted during the early years of the new millennium, when the country received economic sanctions from the global Western countries, it has helped to bridge gap of poverty and underdevelopment as technology of different forms has been adopted in Zimbabwe with the view of enhancing the livelihoods of many Zimbabweans and countering the effects of sanctions amongst many people. Smart thermometers and blood pressure monitoring machines have been adopted more in Zimbabwe, and now people can self-check their temperatures, blood pressure, heart beat at home without even going to the doctor. This has helped a lot, especially for the rural population, where many people live far away from medical facilities like hospitals and clinics. This has led to early detection of a problem and has become a welcome relief for the people, and can also promote accurate self-medication.

Wearable gadgets, such as smart watches, have also become popular amongst many people in

Zimbabwe. Athletes have used these smart watches more often, and currently, the government has vowed to put up more policies that improve the adoption of smart technology amongst many people in Zimbabwe. The government has promised to improve and make free internet access more available to many people, especially in public domains, to improve the usage and popularity of the Internet of Things in Zimbabwe. This will indeed drive the economy further ahead into the digital world by improving access to business platforms. With the majority of the people in the informal sector, smart technology will improve the ways they trade and also enhance the ways of making money. Many people in the small-scale business sector have been importing their products from China, the UK, and the UAE, and thus, the Internet of Things has made it easy for many people to buy goods due to its availability and accessibility.



Challenges are also being witnessed, especially a lack of proper infrastructural development to enable the viability of smart technology, especially in the marginalised areas. In some rural areas, there is difficult phone network connectivity, which also makes it difficult for internet connectivity to be realised. Telone has recently upgraded their wify systems, replacing the fibre network systems that were causing difficulties in connectivity due to constant vandalism, but now the new system is operational only in urban and peri-urban areas where the previous fibre network systems were available. There is a need to roll out more infrastructure to the marginalised areas through the construction of booster networks so that many people can access the internet, which in turn increases adoption of smart technology amongst the people. Econet recently wants to construct a data centre at the Robert Mugabe International Airport in order to increase technological control of data in Zimbabwe. Also, the current government plans to build a new Cyber City in Mt Hampden, with the view to improving the Internet of Things and promoting more usage of smart technology amongst the people. This will increase the education quality and lifestyle in general in a country that is predominantly rural and underdeveloped. In terms of agriculture, the government has introduced smart techniques through the use of drones for agriculture, and this has indeed revolutionised farming, leading to better yields and improved food security. With this, smart technology adoption in Zimbabwe has been on the rise, and it has improved the livelihoods of many people in the country.

SIGNING OFF..

UNTIL WE DEFEND AGAIN

Stay ahead of every threat

Subscribe for exclusive insights, expert analysis, and real time updates on the evolving cybersecurity landscape

@cyberworldinsight