May 2026

CYBER WATCH

CYBER WORLD INSIGHT

VOLUME. 02, ISSUE 12

CENTER OF CYBER WORLD INSIGHT

NATIONAL INTERNATIONAL EMERGING TECH ANALYSIS

TRACKING THREATS. EXPLORING INNOVATION.

May 2026

CYBER WATCH

VOLUME. 02, ISSUE 12

CENTER FOR CYBER WORLD INSIGHT

May 01-15, 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.

May 2026

CYBER WATCH

VOLUME. 02, ISSUE 12

CENTER FOR CYBER WORLD INSIGHT

May 01-15, 2026

FROM THE TEAM

Cyber Security and Emerging Technologies are still at the forefront of global discussion as the digital landscape continues to evolve. In today's world, with the threat of cyber attacks against critical infrastructure and the rapid development of AI, nations and organizations are realizing the value of digital resilience and technological preparedness.

In this issue of Cyber Watch, we cover significant advancements in the cyber space, such as new security threats, national initiatives in AI development, and technology's impact on strategic and institutional frameworks. We have also delved into cutting-edge advancements like wearable medical gear and cutting-edge cybersecurity strategies like Zero Trust Security, which are shaping the future of digital security.In a world of rapid information flow and evolving cyber threats, awareness, preparedness, and innovation continue to be vital.

With this publication, we hope to deliver timely insights, informed perspectives and greater understanding of developments in cyber and technology.

We extend our appreciation to our contributors, editorial team, and readers for their continued support and engagement.

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

Kainat Shahid

CALL FOR PAPERS

We invite researchers, academicians, practitioners, and policymakers to submit original, unpublished research papers for the upcoming Summer Issue of the Journal of Cyber World Insight.

SUBMISSION GUIDELINES

Papers must be original, unpublished, and not under consideration elsewhere.

Follow the journal's formatting.

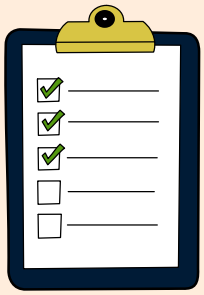
- Word limit: 6000-8000 words (including references).
- File must be in Microsoft Word format (.doc or .docx).
- Abstract: 150-250 words.
- Include 4-6 keywords.

REFERENCES (Any Style)

- You may follow any standard referencing style, including but not limited to: APA MLA Chicago IEEE Harvard OSCOLA.
- Ensure consistency and accuracy in your references.

Exploring the intersection of technology, security, and global politics for a safer and smarter world.

For detailed guidelines, visit our website: www.cyberworldinsight.com/submission-guidelines/



SUBMISSION

Submit your papers via email to: "editor@cyberworldinsight.com"

Please include the subject line: "Submission for Summer Issue - Journal of Cyber World Insight"

SUBMISSION DEADLINE

MAY 31, 2026

May 2026

LATEST CYBER NEWS

VOLUME. 02, ISSUE 12

NATIONAL CERT WARNS OF RISING CYBERATTACK THREATS TO GOVERNMENT DIGITAL INFRASTRUCTURE

The National CERT has warned about increasing threats of cyberattacks targeting government websites and digital platforms. CERT recommended shifting all government websites to “read-only” mode as a preventive security measure.

According to the advisory, authorities were directed to limit access to logins, website modifications, and strengthen database security protocols. The implementation of “read-only” mode would help prevent cyber intrusions and ensure the security of national digital infrastructure. The advisory further stated that such attacks could disrupt government operations and compromise sensitive information of individuals through official contacts and digital systems. These cyberattacks may aim to gain long-term access to government services and websites, create social disruption, or interfere with critical defense infrastructure.

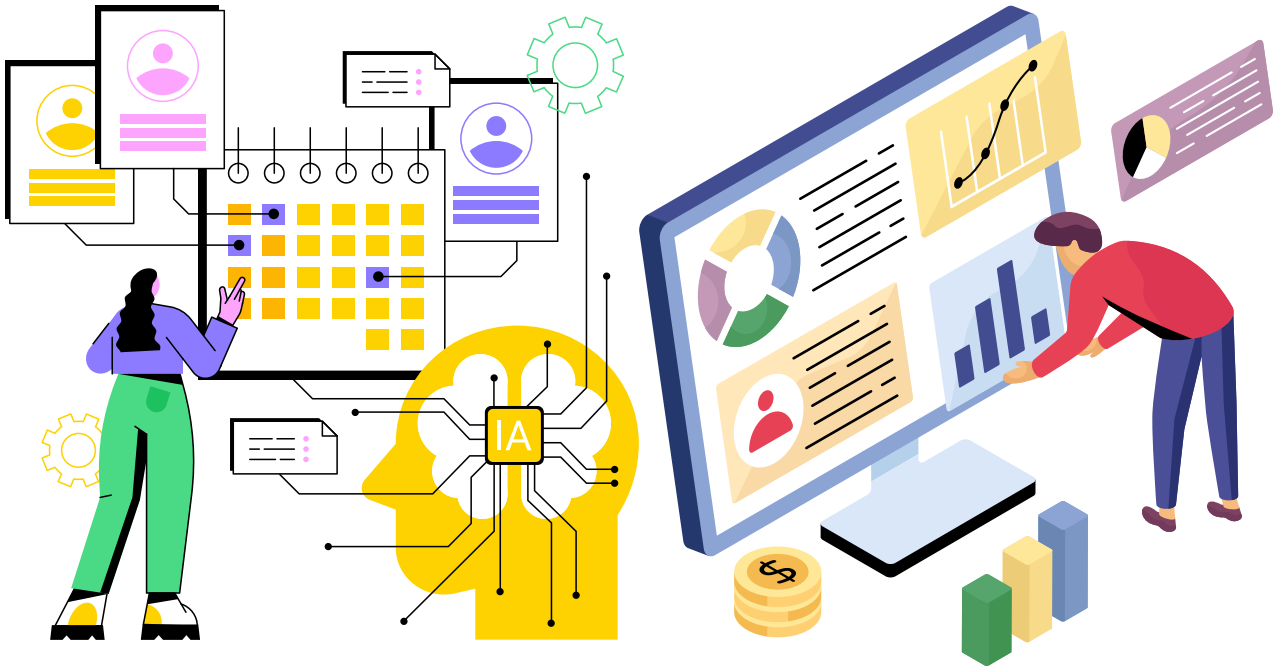
Identifying multiple sources of threats, the National CERT highlighted state-sponsored Advanced Persistent Threat (APT) groups and ideologically driven hacktivists among the key actors behind these activities.

(Source: The News, 2026)

May 2026

LATEST CYBER NEWS

VOLUME. 02, ISSUE 12



GOVT PLANS 20,000 AI TRAINING PROGRAMMES UNDER NATIONAL AI ADVANCEMENT INITIATIVE

The Ministry of IT and Telecommunication plans to launch 20,000 online training programmes in Artificial Intelligence (AI) across the country for fresh graduates, government officials, professionals from various sectors, teachers, and freelancers through an advanced Learning Management System (LMS).

The duration of these training programmes will range from six to twelve months and will be introduced under the National AI Advancement Initiative (NAIAI). The initiative is a strategic national intervention designed to position Pakistan as an emerging player in the global AI landscape.

The programme aims to enhance innovation in both the public and private sectors while aligning with domestic and international market demands. Software and AI expert Asim Tausif stated, “Pakistan's share in the global IT sector currently stands at less than 1%. However, with the rapid transformation driven by AI and related technologies, the country has the potential to secure a significant global position through trained human resources and upgraded infrastructure.”

Many professionals also encouraged such initiatives to help Pakistan adapt to the rapidly advancing global technological environment.

(Source: Tribune, 2026)

WORLD PASSWORD DAY

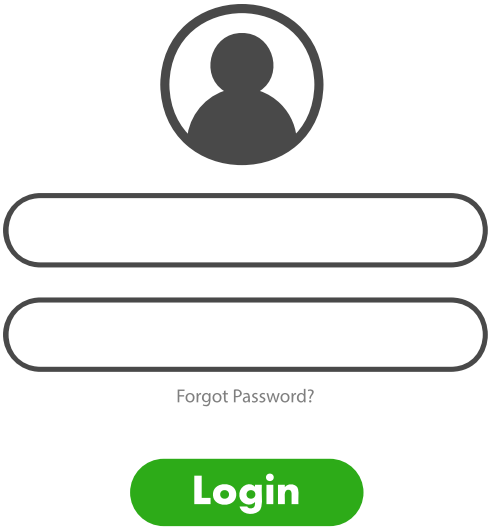
Each year on the first Thursday of May, World Password Day is celebrated as a reminder of the significance of passwords in ensuring cybersecurity. In this digital era, people and businesses depend on online platforms for communication, banking, learning, and conducting business. However, weak passwords and reused passwords remain one of the top reasons for cyber breaches globally.

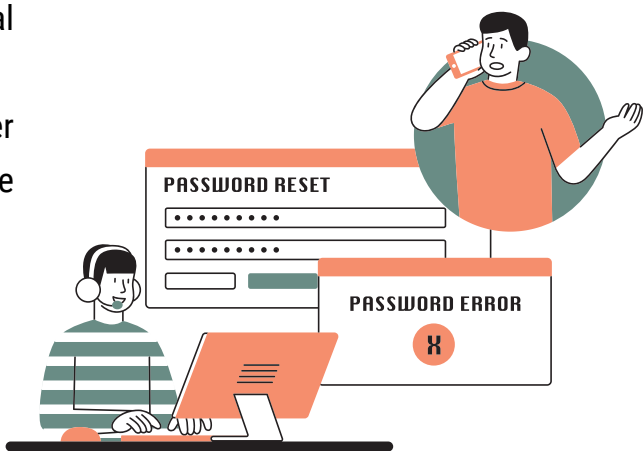
Cybercriminals often exploit simple passwords through phishing attacks, credential stuffing, and brute-force techniques to gain unauthorized access to sensitive information. Cybersecurity experts therefore recommend creating different and complex passwords for each account, and changing them frequently.

Online security practices have become much more robust, with the use of multi-factor authentication (MFA), password managers, and biometric verification. However, raising awareness is still a critical factor in mitigating cyber risk.

World Password Day aims to promote safe digital practices by urging individuals to enhance their online security and recognize the significance of safeguarding personal and organizational information. It also emphasizes the mutual responsibility of persons, companies and institutions to create a safer digital environment.

With the ever-growing threat of cybercrime today, proper password use is among the easiest and most effective measures against this type of crime.



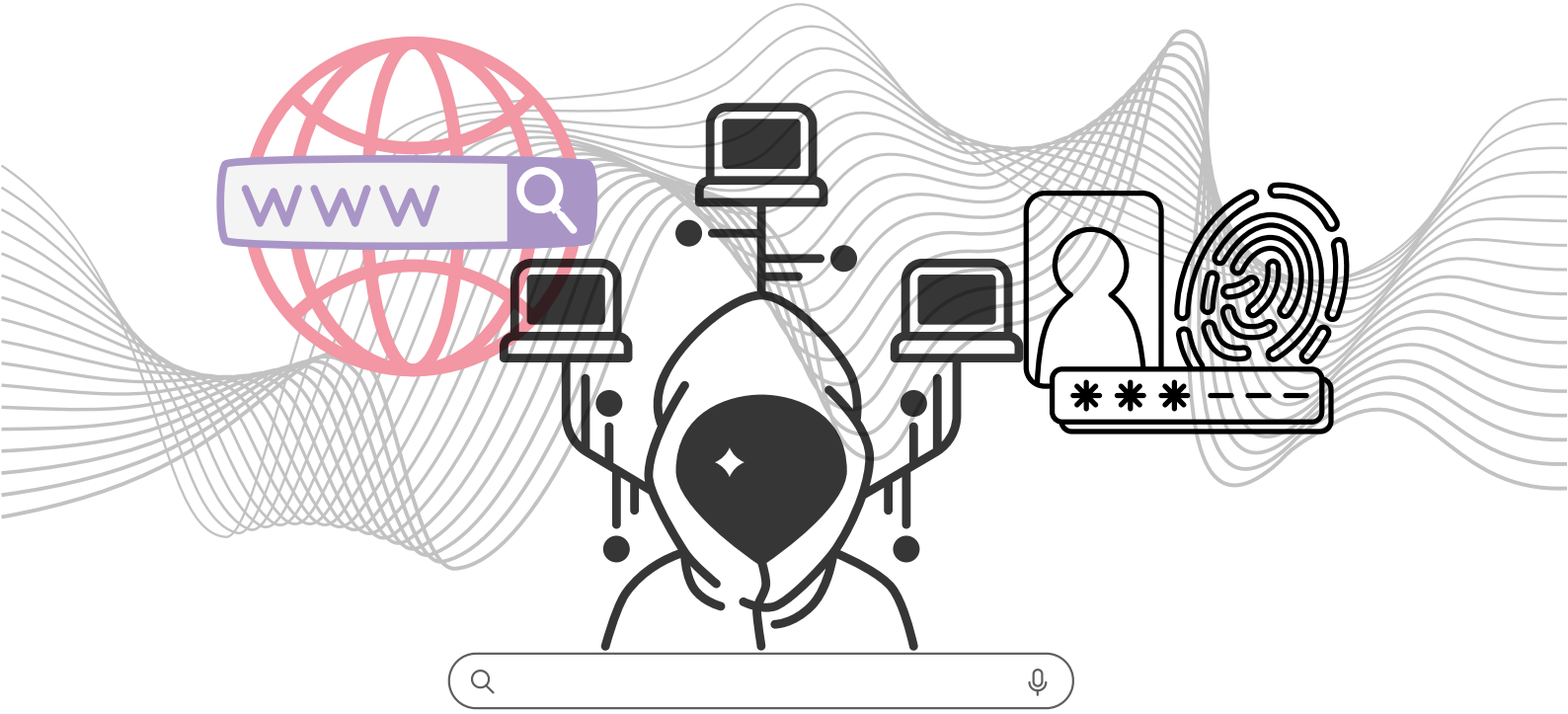


May 2026

LATEST CYBER NEWS

VOLUME. 02, ISSUE 12

GOOGLE UNCOVERS FIRST OF ITS KIND CYBER-ATTACK



In recent cyber-attacks, intelligence was used to discover a previously unknown vulnerability in a computer system. Google's threat analysis team found that some malicious individuals collaborated on using this vulnerability to bypass the authentication mechanism that requires an additional code alongside passwords. These hackers used intelligence to support their coding process during the creation of the cyber-attack on the computer system. This is a deviation from the traditional approach taken by malicious parties to compromise computer systems. spite stopping the attack, Google informed the manufacturer of the software about this vulnerability and encouraged them to rectify it. Some experts observed that there were specific characteristics that suggested that artificial intelligence had been used in the creation of the code for this cyber-attack. The coding process was done using complex codes and having a lot of unnecessary comments within the script. These malicious individuals also fabricated the impact of this cyber-attack. Artificial intelligence is now becoming advanced enough to exploit computer system vulnerabilities beyond the reach of conventional security mechanisms.

(Source: Axios, 2026)

May 2026

LATEST CYBER NEWS

VOLUME. 02, ISSUE 12

GERMANY WARNS OF GROWING AI-DRIVEN CYBER THREATS TO FINANCIAL SECTOR

Germany's financial regulator, the Federal Financial Supervisory Authority also known as BaFin expressed concerns over the cybersecurity threats that come with advanced artificial intelligence systems. BaFin President Mark Branson talked about this in Frankfurt saying that new artificial intelligence models can find weaknesses in new computer systems very quickly. This warning comes after people started paying attention to Anthropics artificial intelligence model, called Mythos.

Cybersecurity experts believe Mythos could be a problem for banks and the security systems they use. Regulators are worried that artificial intelligence technologies like this will help people with malicious intents find and use weaknesses in computer systems faster and on a much larger scale. BaFin is forming a new team to check the cybersecurity of institutions. They are saying that financial institutions need to invest more in protecting themselves from cyber attacks. This is a concern for people all around the world because artificial intelligence is getting better very fast. The Federal Financial Supervisory Authority or BaFin wants to make sure that financial institutions are safe from these threats. Artificial intelligence systems are a part of this and BaFin is taking steps to deal with the risks they pose.

(Source: Reuters, 2026)

May 2026

EMERGING TECH

VOLUME. 02, ISSUE 12

SAMSUNG GALAXY RING

“The Galaxy Ring represents the growing trend of invisible wearable technology, where AI-powered health monitoring is integrated into compact everyday accessories”

The galaxy ring focuses on tracking health and wellness. Its main features include sleep tracking, monitoring heart rate, tracking blood oxygen levels, monitoring temperature, tracking daily activity, moitoring stress, and analysing the individuals energy score

May 2026

EMERGING TECH

VOLUME. 02, ISSUE 12

Material
Titanium frame

Colors
Titanium Black, Titanium Silver, Titanium Gold

Sizes
5–13

Weight
2.3g – 3g

Dimensions
7.0mm × 2.6mm

Water Resistance
IP68 + 10ATM

Connectivity
Bluetooth LE 5.4

Battery Life
Up to 7 days

Sensors
Accelerometer, PPG heart sensor, Skin temperature sensor

May 2026

AI ACROSS DISCIPLINES

VOLUME. 02, ISSUE 12

Zero Trust Security: The Future of Cyber Defense

The threats in the cyber world are continually changing and the conventional security systems have become less and less efficient in protecting against advanced attacks. In the past, the assumption was that anything within a network was safe. But, in today's era of remote working, the cloud, insider threats, and artificial intelligence-powered cyber attacks, it is no longer enough. This is where the Zero Trust Security comes in as a contemporary cybersecurity solution. The core concept of Zero Trust is “Never Trust, Always Verify.” Rather than relying on users or devices to be a trusted part of a network, Zero Trust continually authenticates identities, access privileges, and device security before granting access to sensitive systems or data. Compared to traditional security models which are primarily perimeter-centric, Zero Trust takes a more holistic approach by assuming threats might be

present within the network. This means that all logins, connections to devices, and data requests are monitored and authenticated in real-time.

Key principles of Zero Trust include:

- Multi-factor authentication (MFA)
- Least-privilege access
- Continuous monitoring
- Device verification
- Identity-based security controls

Governments, financial institutions, healthcare organizations and technology firms around the globe are increasingly turning to Zero Trust approaches to bolster digital resilience. Today, Zero Trust is becoming a part of enterprise security solutions provided by major cloud platforms and cybersecurity companies.In the present digital landscape, Zero Trust Security is poised to be a key component of safeguarding digital infrastructure, minimizing data breaches, and ensuring a more secure access to information.The advent of digital technology has seen cybercriminals evolve to new heights and Zero Trust Security is anticipated to be a crucial factor in securing digital infrastructure, data protection, and access to information in the modern world..

May 2026

AI ACROSS DISCIPLINES

VOLUME. 02, ISSUE 12

Social Media & its Impact on Political Agendas

BY FATIMA BATOOL

Trending Politics & the Rise of Digital Influence

Over the past few years, social media has evolved beyond a personal communication tool to one of the most influential ones that define the political agenda around the world. X (previously Twitter), Facebook, Instagram, and Tik Tok are no longer just a reflection of political discourse, but they are its creators. Online trends, viral stories, and even algorithmic visibility are having an increasing impact on political priorities, popular discourse, and even state policies. Although social media has democratized the political process, it has also brought about serious doubts in terms of manipulation, polarization and undermining of informed decision making.

In its most basic form, political agenda-setting denotes the possibility of impacting the priorities of what issues are taken to be discussed publicly and by the government. In earlier days, it was the political elites, mainstream media and formal institutions that held this position. The social media is however, today disrupting this hierarchy. Hashtags have the potential to bring marginal issues to national attention in a few hours necessitating a political response. The examples of online mobilization in terms of movements, including the Arab Spring, the Me Too, and Black Lives Matter, show that they can re-establish the political priorities and force governments to take such issues into consideration that they might have not done before.

Social Media as a Democratic Force

This change has certainly increased the political involvement. The prevailing citizens who were earlier marginalized in official political activities now have arenas to express their views, engage in demonstrations, and confront government. The social media reduces entry barriers, which means that the youth, minorities, and civil society groups can affect the political discourse. In this aspect, the social media enhances democratic participation by giving more voices than conventional (traditional) authority systems.

There is however a lot of danger in this empowerment. The policy agendas that are formed on social media may not necessarily have to be relevant to policy and aligned with the interests of the nation in the long-term, but rather be visible and emotional. Algorithms are based on the idea that content that will be liked, shared, and comment on is given a priority instead of accuracy or depth. Consequently, dramaticism often relegates serious debate. Policy problems are simplified to slogans, whereas subtle debates are difficult to propagate.

The Risk of Algorithmic Politics

Besides, the rate of information spreading via the internet does not give a lot of chances to verify it. Disinformation and misinformation campaigns have emerged as potent instruments in the creation of political agendas especially during elections. Once a fake story has gone viral, it will affect the mass consciousness quicker than the fact-checking systems will react. The case of the Cambridge Analytica scandal and reported incidences of political interference by other countries in elections underlines how the social media can be used to trigger political

behaviour and the agenda-setting processes.

Political polarization is another important issue. The social media networks tend to provide social media echo chambers where users are only exposed to the social media opinions that support their already held beliefs. This strengthens ideological differences and diminishes the chances of agreement. The political agendas that would arise in such settings are confrontational as opposed to cooperative and focus more on identity politics instead of policy solutions. This process may destroy the democratic institutions and social cohesion in highly polarized societies.

Even governments and political actors have gone to this new reality. Social media are becoming a major means through which political leaders bypass the traditional media, direct messages to the citizens, and position issues in their own terms. Although such direct communication may increase transparency, it enables leaders to filter messages, avoid criticism, and encourage their supporters using emotionally charged messages. Political agendas are thus potentially to turn into personality agendas instead of becoming policy-driven.

Other people even believe that social media does not divide society; it only mirrors it. Although this point of view is partially correct, it underrates the fact that digital platforms enhance some narratives and restrain others. The social media architecture, its algorithms, monetization frameworks, and content moderation practices influence the formation of the electorally significant. In this respect, social media is not a neutral territory but an influential political force itself.

The effect of social media on the political agenda is especially high in developing nations, where institutional distrust might not be strong yet, and regulatory structures can be weak. In this kind of environment, unregulated digital power may enhance political instability, cultivate extremist ideas, and weaken government. Meanwhile, such platforms are also indispensable instruments of civic engagement and accountability, and unconditional restrictions are not only impossible but also undesirable.

Balancing Freedom & Responsibility

The issue is maintaining freedom of expression and responsibility, therefore. The governments, technology corporations, and civil society should cooperate to facilitate digital literacy, augment the fact-checking systems, and implement more transparency in the algorithm decision-making. It is also important that the political actors should understand that the agenda-setting that can be caused by online trends should not be an alternative to the use of evidence-based policymaking.

To sum up, social media has radically transformed the political agenda-setting paradigm. Its created new ways in which people can be politically engaged. It has, however, also made some parts more polarized, allowed manipulation, and put more emphasis on appearance than content. As politics increasingly moves into the digital world, the real question is no longer whether social media has made citizens more powerful or whether it is a political tool. It clearly has changed traditional centres of power. The important question now is how societies will manage and respond to the influence and power of social media in politics. It is quite possible that the future of democratic governance rests on how well we can use the potential of social media without giving up political judgment to algorithms

May 2026

AI ACROSS DISCIPLINES

VOLUME. 02, ISSUE 12

UNESCO Global Al Governance Framework: What Developing Nations Agreed To

BY HADIA SARWAR

Machine intelligence is no longer just a concept in science fiction or research labs. Today, it shapes how people study, work, communicate, shop, and think. From biometric, identification and decision automation, technology is becoming part of everyday life worldwide. But as artificial intelligence becomes more powerful, another important question occurs: who will control it, and how can it be used maturely?

This concern took center stage during UNESCO's discussions on the Global AI Governance Framework, where developing nations joined larger global powers to agree on moral standards for artificial intelligence. According to UNESCO's Recommendation on the Ethics of Artificial Intelligence, AI should benefit humanity by protecting human rights, honor, and equality. UNESCO highlights that "**AI must work for humanity, not the other way around**." This message functioned as the foundation of the agreement.

The significance of this framework depends not only on the participation of great powers but also in the strong involvement of emerging economies. Countries from Asia, Africa, and Latin America recognized that machine intelligence could either be a tool for progress or a source of disparity. For many of these nations, the debate was not just about innovation, it was about fairness, embodiment, and endurance in a cyberspace heavily influenced by industrialized nation.

One key issue among developing nations is that machine intelligence systems are often created using data and western outlooks. As mentioned in UNESCO reports and policy discussions, unfair systems can impact hiring systems, law enforcement tech, banking services, and online platforms. A system created without understanding local languages, cultures, or economic realities may unconsciously differentiate against millions of people in poorer regions.

This is why developing nations strongly supported the principle administration rather than unchecked technology race. UNESCO's framework emphasizes accountability, privacy protection, and acceptance as essential principles. These values may seem technical in policy documents, but they directly affect everyday people. Such as a student applying for a scholarship, a worker looking for a job, or a citizen engaging with digital government

systems could all be affected by artificial intelligence's decisions in the future. Another major issue raised during the negotiations was the increasing digital divide between rich and poor countries

From a political perspective, the agreement reflects a global transformation. Technology is becoming a form of power. Countries that lead in artificial intelligence may eventually influence economies, global security, and public opinion across borders. Developing nations are aware of this shift. Their involvement in UNESCO's framework was a way to guarantee that future smart technology regulations are not dictated solely by a few wealthy states or powerful tech companies.

However, there are doubts about how successful these agreements will be. Analysts suggest that international frameworks may sound promising but struggle during fulfillment. Many modernized countries still lack strong institutions, technical expertise, or financial resources to effectively regulate ai systems. Large tech corporations also continue to hold significant influence over artificial intelligence development worldwide.

Still, defusing the framework completely would overlook its broader importance. Global agreements often start with shared principles before becoming stronger over time. Human rights agreements and international laws began with discussions that many initially saw as symbolic. UNESCO's AI governance framework may sound like a similar first step toward global accountability in the digital age.

Perhaps the most important aspect of this agreement is the changing perspectives of developing nations. Instead of being passive users of foreign technology, many countries are now insisting on a role in deciding how these systems operate. They realised that dependence on technology can easily lead to a new form of inequality in today's world.

UNESCO's Recommendation on the Ethics of Artificial Intelligence and related policy discussions state that principled AI governance is necessary to ensure technological progress does not undermine human dignity or social justice. In many respects, this framework is not just about regulating machines; it is about protecting people.

As machine technology continues to reshape economies, governments, and daily human activities, developing nations are making it transparent that they no longer intend to be silent spectators in a technology running world. The debate is no longer just about innovation or technological progress, it is about power, equality, and the kind of future humanity wants to create. If AI is going to impact billions of lives globally, the voices of poorer and developing nations must be heard. The rising question now is, will the tomorrow of artificial intelligence be shaped only by those powerful enough to create it, or by all those whose lives will automatically be affected by it?

May 2026

AI ACROSS DISCIPLINES

VOLUME. 02, ISSUE 12

CHATBOTS AND DIGITAL ASSISTANTS IN LOCAL LANGUAGES

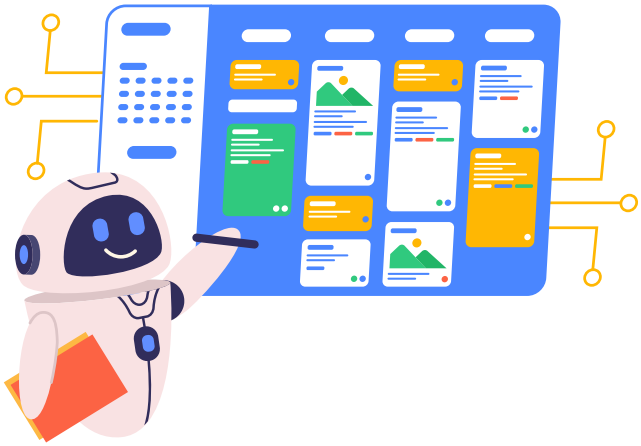
BY GODFREY MASAWI

Chatbots and digital assistants have made communication and daily life considerably easier for millions of people, driving their rapid adoption across the globe — particularly in customer care, banking, and other essential services. In Africa, their impact has been especially significant, enabling cardless financial transactions and opening digital platforms to communities that were previously excluded.

Among those who have benefited most are the elderly and the less literate, who now find it easier to navigate mobile banking and purchase mobile data independently. In a continent home to hundreds of ethnic groups and languages, chatbots have proven invaluable by communicating in mother tongues and indigenous languages, making services accessible and allowing people to raise concerns in the language most natural to them.

In Zimbabwe, chatbots have become widely used for communicating with mobile network providers when errors occur. Through e-commerce chatbots, tracking of sent goods has become straightforward — particularly for people living in the diaspora. Remittance platforms have similarly benefited, with chatbots guiding users through the process of retrieving and processing funds. In South Africa, where many indigenous people prefer their local languages, chatbots have enabled clearer communication for those who struggle with English due to limited formal education.

Virtual assistants, too, have expanded access by operating in local languages, narrowing the gap between rural and urban communities. Tasks such as booking appointments and checking account



balances can now be completed in familiar tongues. In conflict-affected areas, virtual assistants have played a meaningful role in alerting communities to dangers and advising on how risks can be mitigated. Banking bots have further transformed the financial lives of many Africans, with companies such as Econet and Old Mutual in Zimbabwe investing in these tools to improve efficiency and reach a broader customer base.

During the COVID-19 pandemic, chatbots proved critical for information dissemination and the reporting of infections and deaths, especially in marginalised regions. Toll-free numbers leveraging local languages helped channel vital information to the appropriate health and government organisations, contributing to efforts to contain the spread of the virus. Citizens also used these platforms to report illegal public gatherings, supporting government enforcement and securitisation measures. Among digital assistants, Google Assistant stands out for its versatility offering voice search functionality and deep integration with Chrome devices for a seamless experience.

Despite these achievements, significant challenges remain. Improving the accuracy and quality of information delivered through these platforms is an ongoing concern, and the availability of dialectal variations across the full spectrum of local languages is still limited. Dominant languages tend to receive the most attention, leaving speakers of minority languages underserved. For these tools to fulfil their potential, particularly for educational purposes wider linguistic coverage is essential.

Overall, chatbots and digital assistants have brought tangible improvements to people's lives across Africa. By communicating in local languages, they have made services more inclusive and accessible, and their continued development holds real promise for communities long left behind by the digital age.

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